

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

-v-

JOSHUA ADAM SCHULTE,

Defendant.

Filed with the Classified
Information Security Officer
CISO 
Date 1/28/22

83 17 Cr. 548 (JMF)

REDACTED / CLEARED FOR PUBLIC RELEASE

MOTION

- (1) TO SUPPRESS EVIDENCE SEIZED FROM GOOGLE, GITHUB, AND REDDIT;**
- (2) FOR SEVERANCE / BIFURCATION OF TRIAL;**
- (3) TO PRECLUDE THE GOVERNMENT FROM INTRODUCING TESTIMONY OR EXHIBITS DERIVED FROM THE FORENSIC CRIME SCENE DENIED TO THE DEFENSE;**
- (4) TO COMPEL CLASSIFIED DISCOVERY;**
- (5) TO SUPPRESS NON-RESPONSIVE AND ATTORNEY-CLIENT PRIVILEGED DOCUMENTS SEIZED FROM MCC**

Joshua Adam Schulte
Slave #79471054
Metropolitan Detention Center (MDC)
P.O. Box 329002
Brooklyn, NY 11232

TABLE OF CONTENTS

| | |
|--|----|
| I. TABLE OF AUTHORITIES..... | iv |
| II. MOTION TO SUPPRESS GOOGLE/REDDIT/GITHUB SEARCH WARRANT..... | 1 |
| A. The search warrant application failed to establish a minimum nexus between the alleged offense and the online accounts..... | 1 |
| 1. Probable cause to arrest is not sufficient to conduct a search..... | 2 |
| 2. The affidavit contained no factual allegations connecting the alleged offenses to Mr. Schulte's online accounts..... | 3 |
| 3. Conclusory statements based on "training and experience" do not magically transform an arrest warrant into a search warrant..... | 7 |
| 4. The allegations concerning the theft of national defense information in March 2016 were too stale to justify searching Mr. Schulte's online accounts a full year later in March 2017..... | 10 |
| 5. Given the totality of the circumstances, Donaldson's warrant failed to establish the necessary nexus between the alleged crime and Mr. Schulte's online accounts..... | 12 |
| B. The search warrant application was insufficiently particular, overbroad, and authorized a general warrant..... | 15 |
| 1. Agent Donaldson sought a general warrant to seize Mr. Schulte's entire electronic footprint since birth..... | 16 |
| 2. The special privacy concerns that apply to the search of personal electronic data and the particularity requirement..... | 16 |
| 3. The Donaldson warrant was insufficiently particular as it was broader than justifiable by the probable cause upon which the warrant was based..... | 22 |
| C. The good-faith exception to the exclusionary rule does not apply..... | 25 |
| III. MOTION FOR SEVERANCE / BIFURCATION..... | 29 |
| A. The MCC counts are improperly joined with the WikiLeaks counts and should be severed..... | 29 |

| | |
|--|----|
| B. Trial should be severed so Mr. Schulte can pursue a speedy trial of the MCC Counts that are used to justify SAMs and indefinite torture | 33 |
| C. Alternatively, the MCC counts should be bifurcated from the WikiLeaks counts to prevent substantial prejudice to Mr. Schulte..... | 33 |
| 1. Juror knowledge of Mr. Schulte's pre-trial detention violates Due Process | 35 |
| 2. Vast differences between the WikiLeaks counts and MCC counts would lead to juror confusion and unfair prejudice | 36 |
| 3. Mr. Schulte has strong reasons to testify in his defense on the WikiLeaks counts and not for the MCC counts | 39 |
| IV. MOTION TO PRECLUDE GOVERNMENT FROM INTRODUCING TESTIMONY OR EVIDENCE DERIVED FROM FORENSIC CRIME SCENE DENIED TO DEFENSE..... | 40 |
| A. The Due Process Clause of the Fifth Amendment compels the government to provide equal access to private experts retained by the defense just as it does for its own experts | 41 |
| B. The Confrontation Clause of the Sixth Amendment..... | 44 |
| V. MOTION TO COMPEL CLASSIFIED DISCOVERY | 46 |
| A. Applicable Law | 47 |
| B. Access to stolen CIA Backups | 48 |
| C. Access to CIA emails and Sametime messages sent and received by Mr. Schulte, including all metadata..... | 51 |
| D. Access to CIA Polygraph and results..... | 52 |
| VI. MOTION TO SUPPRESS NON-RESPONSIVE DOCUMENTS SEIZED FROM MCC AND ATTORNEY-CLIENT PRIVILEGED DOCUMENTS..... | 52 |
| A. Attorney-Client Privilege | 53 |
| B. Seizure and search of Non-Responsive documents | 54 |
| C. Suppression of specific documents | 55 |
| 1. Malware of the Mind..... | 56 |
| 2. Red notebook labeled "7/25 -9/" | 61 |

| | |
|--------------------------|----|
| 3. Other Notebooks | 64 |
| VII. CONCLUSION | 65 |

I. TABLE OF AUTHORITIES

Cases

| | |
|---|----|
| <i>ACLU v. NSA</i> , 925 F.3d 576 (2d Cir. 2019) | 53 |
| <i>Ake v. Oklahoma</i> , 470 U.S. 68 (1985) | 44 |
| <i>Andresen v. Maryland</i> , 427 U.S. 463 (1976) | 54 |
| <i>Arizona v. Grant</i> , 556 U.S. 332 (2009) | 15 |
| <i>Ayeni v. Mottola</i> , 35 F.3d 680 (2d Cir. 1994) | 15 |
| <i>Barnard v. Henderson</i> , 514 F.2d 744 (5th Cir. 1975) | 41 |
| <i>Bernbach v. Timex Corp.</i> , 174 F.R.D. 9 (D. Conn. 1997) | 59 |
| <i>Boyd v. United States</i> , 116 U.S. 616 (1886) | 53 |
| <i>Brady v. Maryland</i> , 373 U.S. 83 (1963) | 48 |
| <i>Brigham City v. Stuart</i> , 547 U.S. 398 (2006) | 4 |
| <i>Camara v. Municipal Court of City and County of San Francisco</i> , 387 U.S. 523 (1967) | 8 |
| <i>Carpenter v. United States</i> , 138 S. Ct. 2206 (2017) | 8 |
| <i>Chambers v. Mississippi</i> , 410 U.S. 284 (1973) | 48 |

| | |
|---|-------|
| <i>Clark v. Buffalo Wire Works Co.,</i> 190 F.R.D. 93 (W.D.N.Y. 1999) | 59 |
| <i>Coolidge v. New Hampshire,</i> 403 U.S. 443 (1971)..... | 22 |
| <i>Cross v. United States,</i> 335 F.2d 987 (D.C. Cir. 1964)..... | 39 |
| <i>Davis v. Goora,</i> 320 F.3d 346 (2d Cir. 2003) | 60 |
| <i>Davis v. United States,</i> 564 U.S. 229 (2011)..... | 28 |
| <i>Deck v. Missouri,</i> 544 U.S. 622 (2005)..... | 35 |
| <i>Estelle v. Williams,</i> 425 U.S. 501 (1976)..... | 35 |
| <i>Pharmacy Records v. Nassar,</i> 379 Fed. Appx. 522 (6 th Cir. 2010)..... | 46 |
| <i>Fisher v. United States,</i> 425 U.S. 391 (1976)..... | 59 |
| <i>Go-Bart Importing Co. v. United States,</i> 282 U.S. 344, 357 (1931)..... | 23 |
| <i>Gomez v. Vernon,</i> 255 F.3d 1118 (9th Cir. 2001) | 54 |
| <i>Groh v. Ramirez,</i> 540 U.S. 551 (2004)..... | 3, 25 |
| <i>Hawkins v. United States,</i> 358 U.S. 74 (1958)..... | 48 |
| <i>Herring v. United States,</i> 555 U.S. 135 (2009)..... | 25 |

| | |
|--|------------|
| <i>Illinois v. Gates</i> , 462 U.S. 213 (1983)..... | 1, 4, 7, 8 |
| <i>In re 650 Fifth Ave. & Related Props.</i> , 830 F.3d 66 (2d Cir. 2016) | 23 |
| <i>In re Horowitz</i> , 482 F.2d 72 (2d Cir. 1973) | 59 |
| <i>In re Terrorist Bombings of U.S. Embassies in E. Africa</i> , 552 F.3d 93 (2d Cir. 2008) | 47 |
| <i>Jenkins v. Anderson</i> , 447 U.S. 231 (1980) | 40 |
| <i>Jones v. United States</i> , 362 U.S. 257 (1960) | 1 |
| <i>Kentucky v. King</i> , 563 U.S. 452 (2011) | 22, 54 |
| <i>Lauro v. Charles</i> , 219 F.3d 202 (2d Cir. 2000) | 15 |
| <i>Loughrin v. United States</i> , 134 S. Ct. 2384 (2014) | 60 |
| <i>Marron v. United States</i> , 275 U.S. 192 (1927) | 54 |
| <i>Maryland v. Garrison</i> , 480 U.S. 79 (1987) | 22 |
| <i>Massachusetts v. Upton</i> , 466 U.S. 727 (1984) | 7 |
| <i>Massiah v. United States</i> , 377 U.S. 201 (1964) | 61 |
| <i>McDonald v. United States</i> , 335 U.S. 451 (1948) | 3 |

| | |
|--|------------|
| <i>Nathanson v. United States</i> , 290 U.S. 41 (1933)..... | 1, 26 |
| <i>Payton v. New York</i> , 445 U.S. 573 (1980)..... | 15, 54 |
| <i>Pritchard v. County of Erie (In re County of Erie)</i> , 473 F.3d 413 (2d Cir. 2007) | 53 |
| <i>Reynolds v. United States</i> , 345 U.S. 1 (1953)..... | 48 |
| <i>Riley v. California</i> , 573 U.S. 373 (2014)..... | passim |
| <i>Roviaro v. United States</i> , 353 U.S. 53 (1957)..... | 40, 47 |
| <i>Sallier v. Brooks</i> , 343 F.3d 868 (6th Cir. 2003) | 60 |
| <i>Stanford v. Texas</i> , 379 U.S. 476 (1965)..... | 22, 54 |
| <i>Steagald v. United States</i> , 451 U.S. 204 (1981)..... | 2, 3, 54 |
| <i>United States v. Abu-Jihad</i> , 630 F.3d 102 (2d Cir. 2010) | 47 |
| <i>United States v. Alverado</i> , No. 92 CR. 728 (LMM), 1994 WL 669968 (S.D.N.Y. Nov. 30, 1994)..... | 37 |
| <i>United States v. Aref</i> , 533 F.3d 72 (2d Cir. 2008) | 40, 47, 48 |
| <i>United States v. Bain</i> , 874 F.3d 1 (1 st Cir. 2017)..... | 14 |
| <i>United States v. Benevento</i> , 836 F.2d 60 (2d Cir. 1987) | 14 |

| | |
|---|----------------|
| <i>United States v. Brown</i> , 828 F.3d 375 (6 th Cir. 2016) | 2, 14, 26 |
| <i>United States v. Buck</i> , 813 F.2d 588 (2d Cir. 1987) | 23 |
| <i>United States v. Burgess</i> , 576 F.3d 1078 (10 th Cir. 2009) | 24 |
| <i>United States v. Christlan</i> , 893 F.3d 846 (6 th Cir. 2018) | 9 |
| <i>United States v. Clark</i> , 638 F.3d 89 (2d Cir. 2011) | 12, 26, 27 |
| <i>United States v. Comprehensive Drug Testing, Inc.</i> , 621 F.3d 1162 (9 th Cir. 2010) | 16 |
| <i>United States v. Deandrade</i> , 600 F.3d 115 (2d Cir. 2010) | 36 |
| <i>United States v. Defonte</i> , 441 F.3d 92 (2d Cir. 2006) | 53, 59 |
| <i>United States v. Dzialak</i> , 441 F.2d 212 (2d Cir. 1971) | 55 |
| <i>United States v. Ezeobi</i> , No. 10 CR. 669 DLC, 2011 WL 3625662 (S.D.N.Y. Aug. 17, 2011) | 30, 36 |
| <i>United States v. Fernandez</i> , 913 F.2d 148 (4 th Cir. 1990) | 47 |
| <i>United States v. Finazzo</i> , 682 Fed. Appx. 6 (2d Cir. 2017) | 53 |
| <i>United States v. Galpin</i> , 720 F.3d 436 (2d Cir. 2013) | 15, 20, 22, 23 |
| <i>United States v. Gantlas</i> , 824 F.3d 199 (2d Cir. 2016) | 17, 44, 45, 46 |

| | |
|--|--------|
| <i>United States v. George</i> , 975 F.2d 72 (2d Cir. 1992) | 22 |
| <i>United States v. Ginsberg</i> , 758 F.2d 823 (2d Cir. 1985) | 61 |
| <i>United States v. Gomez</i> , 652 F. Supp. 461 (E.D.N.Y. 1987) | 9 |
| <i>United States v. Gonzales</i> , 399 F.3d 1225 (10 th Cir. 2005) | 27 |
| <i>United States v. Griffith</i> , 867 F.3d 1265 (D.C. Cir. 2017) | passim |
| <i>United States v. Grubbs</i> , 547 U.S. 90 (2006) | 10 |
| <i>United States v. Guzman</i> , No. 97 Cr. 786 (SAS), 1998 WL 61850 (S.D.N.Y. Feb. 13, 1998) | 9 |
| <i>United States v. Halper</i> , 590 F.2d 422 (2d Cir. 1978) | 34, 37 |
| <i>United States v. Harris</i> , 805 F. Supp. 166 (S.D.N.Y. 1992) | 37, 39 |
| <i>United States v. Haynes</i> , 729 F.3d 178 (2d Cir. 2013) | 35 |
| <i>United States v. Jacobs</i> , 117 F.3d 82 (2d Cir. 1997) | 60 |
| <i>United States v. Kerik</i> , 615 F. Supp. 2d 256 (S.D.N.Y. 2009) | 30 |
| <i>United States v. Kortright</i> , No. 10 Cr. 937 (KNW), 2011 WL 4406352 (S.D.N.Y. Sept. 13, 2011) | 14 |
| <i>United States v. Krug</i> , 198 F. Supp. 3d 235 (W.D.N.Y. 2016) | 39 |

| | |
|---|---------------|
| <i>United States v. Lahey</i> , 967 F. Supp. 2d 698 (S.D.N.Y. 2013) | 14 |
| <i>United States v. Laury</i> , 985 F.2d 1293 (5 th Cir. 1993) | 28 |
| <i>United States v. Leary</i> , 846 F.2d 592 (10 th Cir. 1988) | 28 |
| <i>United States v. Leon</i> , 468 U.S. 897 (1984) | 7, 25, 26, 27 |
| <i>United States v. Longo</i> , 70 F. Supp. 2d 225 (W.D.N.Y. 1999) | 61 |
| <i>United States v. Lotsch</i> , 102 F.2d 35 (2d Cir. 1939) | 34 |
| <i>United States v. Lucarz</i> , 430 F.2d 1051 (9 th Cir. 1970) | 2 |
| <i>United States v. Martinez</i> , 92-CR-839(SWK), 1993 WL 322768 (S.D.N.Y. Aug. 19, 1993) | 31 |
| <i>United States v. Matias</i> , 836 F.2d 744 (2d Cir. 1988) | 55 |
| <i>United States v. McGrath</i> , 622 F.2d 36 (2d Cir. 1980) | 10 |
| <i>United States v. McPhearson</i> , 469 F.3d 518 (6th Cir. 2006) | 26, 28 |
| <i>United States v. Mejia</i> , 448 F.3d 436 (D.C. Cir. 2006) | 48, 53, 59 |
| <i>United States v. Mejia</i> , 655 F.3d 126 (2d Cir. 2011) | 53 |
| <i>United States v. Moore</i> , 968 F.2d 216 (2d Cir. 1992) | 26 |

| | |
|--|------------|
| <i>United States v. Moran</i> , 349 F. Supp. 2d 425 (N.D.N.Y. 2005)..... | 14 |
| <i>United States v. Morton</i> , 984 F.3d 421 (5 th Cir. 2021) | 21, 23 |
| <i>United States v. Nixon</i> , 418 U.S. 683 (1974)..... | 43 |
| <i>United States v. Oaks</i> , 285 F.Supp.3d 876 (D. Md. 2018)..... | 31 |
| <i>United States v. Ortiz</i> , 857 F.2d 900 (2d Cir. 1988) | 38 |
| <i>United States v. Pabon</i> , 871 F.3d 164 (2d Cir. 2017) | 3 |
| <i>United States v. Paul</i> , 692 F. Supp. 186 (S.D.N.Y. 1988) | 12 |
| <i>United States v. Purcell</i> , 967 F.3d 159 (2d Cir. 2020) | 22 |
| <i>United States v. Raymonda</i> , 780 F.3d 105 (2d Cir. 2015) | 4, 10 |
| <i>United States v. Reilly</i> , 76 F.3d 1271 (2d Cir. 1996) | 24, 27, 28 |
| <i>United States v. Rettig</i> , 589 F.2d 418 (9 th Cir. 1978) | 28 |
| <i>United States v. Rios</i> , 881 F. Supp. 772 (D. Conn. 1995)..... | 9 |
| <i>United States v. Rissew</i> , 580 Fed. Appx. 35 (2d Cir. 2014)..... | 26 |
| <i>United States v. Rivera</i> , 546 F.3d 245 (2d Cir. 2008) | 30 |

| | |
|--|-----------|
| <i>United States v. Rivera</i> , 825 F.3d 59 (1 st Cir. 2016)..... | 12 |
| <i>United States v. Roman</i> , 942 F.3d 43 (1 st Cir. 2019)..... | 9, 15, 28 |
| <i>United States v. Rosa</i> , 626 F.3d 56 (2d Cir. 2010) | 25 |
| <i>United States v. Sampson</i> , 385 F.3d 183 (2d Cir. 2004) | 38, 39 |
| <i>United States v. Schultz</i> , 14 F.3d 1093 (6 th Cir. 1994) | 9 |
| <i>United States v. Shellef</i> , 507 F.3d 82 (2d Cir. 2007) | 30, 31 |
| <i>United States v. Shi Yan Liu</i> , 239 F.3d 138 (2d Cir. 2000) | 28 |
| <i>United States v. Shrake</i> , 515 F.3d 743 (7 th Cir. 2008) | 41 |
| <i>United States v. Singh</i> , 390 F.3d 168 (2d Cir. 2004) | 12 |
| <i>United States v. Smith</i> , 967 F.3d 198 (2d Cir. 2020) | 17 |
| <i>United States v. Tamura</i> , 694 F.2d 591 (9 th Cir. 1982) | 54 |
| <i>United States v. Travlsano</i> , 724 F.2d 341 (2d Cir. 1983) | 1 |
| <i>United States v. Tubol</i> , 191 F.3d 88 (2d Cir. 1999) | 33 |
| <i>United States v. Valenzuela</i> , 596 F.2d 824 (9 th Cir. 1979) | 3 |

| | |
|--|------------|
| <i>United States v. Voustianlouk</i> , 685 F.3d 206 (2d Cir. 2012) | 3 |
| <i>United States v. Wagner</i> , 989 F.2d 69 (2d Cir. 1993) | 10 |
| <i>United States v. Werner</i> , 620 F.2d 922 (2d Cir. 1980) | 29, 33, 34 |
| <i>United States v. Wey</i> , 256 F. Supp. 3d 355 (S.D.N.Y. 2017) | 24 |
| <i>United States v. Wilhelm</i> , 80 F.3d 116 (4 th Cir. 1996) | 27 |
| <i>United States v. Zanzardino</i> , 833 F. Supp. 429 (S.D.N.Y. 1993) | 44 |
| <i>Upjohn Co. v. United States</i> , 449 U.S. 383 (1981) | 53 |
| <i>Walczyk v. Rio</i> , 496 F.3d 139 (2d Cir. 2007) | 12 |
| <i>Warden, Md. Penitentiary v. Hayden</i> , 387 U.S. 294 (1967) | 3 |
| <i>Wardius v. Oregon</i> , 412 U.S. 470 (1973) | 41 |
| <i>Washington v. Texas</i> , 388 U.S. 14 (1967) | 48 |
| <i>Zurcher v. Stanford Daily</i> , 436 U.S. 547 (1978) | 1 |

Statutes

| | |
|--------------------------|--------|
| 18 U.S.C. § 793(e) | 36 |
| 18 U.S.C. APP. 3 | 46, 47 |

Rules

| | |
|-------------------------------|------------|
| Fed. R. Crim. P. 08(a) | 29, 33, 37 |
| Fed. R. Crim. P. 14 | passim |
| Fed. R. Crim. P. 14(a) | 33 |
| Fed. R. Crim. P. 16 | 40, 48 |
| Fed. R. Crim. P. 16(F) | 52 |
| Fed. R. Evid. 403 | 38, 39 |
| Fed. R. Evid. 404(b) | 38, 39 |
| Fed. R. Evid. 404(b)(2) | 38 |

Constitutional Provisions

| | |
|-----------------------------|----------------|
| U.S. Const. amend. I | 32, 34, 37, 64 |
| U.S. Const. amend. IV | passim |
| U.S. Const. amend. V | 40, 41 |
| U.S. Const. amend. VI | 40, 44, 61 |

Other Authorities

| | |
|--|----|
| 2 Wayne R. LaFare, <i>Search and Seizure</i> § 3.7(a) (5 th ed. 2016) | 12 |
| 2 Wayne R. LaFare, <i>Search and Seizure</i> § 4.6(a) (5 th ed. 2012) | 23 |
| Daniel B. Garrie & Francis M. Allegra, Fed. Judicial Ctr., <i>Understanding Software, the Internet, Mobile Computing, and the Cloud: A Guide for Judges</i> 39, 40 (2015)..... | 45 |
| Boghan Casey, <i>Digital Evidence and Computer Crime</i> 507 (3d ed. 2011)..... | 45 |
| Jim Kerstetter, <i>Microsoft Goes on Offensive Against Justice Department</i> , N.Y. Times (Apr. 15, 2016)..... | 20 |

II. MOTION TO SUPPRESS GOOGLE/REDDIT/GITHUB SEARCH WARRANT

Mr. Schulte previously filed a motion to suppress evidence seized from the March 13, 2017 search of his apartment on July 3, 2019 (Dkt. 108). The district court denied the motion on October 31, 2019 (Dkt. 168). The instant motion challenges the constitutionality of the Google, Reddit, and GitHub warrants that were issued on March 14, 2017. Ex. A. While the underlying basis for probable cause in these warrants is identical, the instant motion challenges whether the warrant establishes the minimal factual nexus between the alleged offense and the online accounts to search; and whether the warrants were sufficiently particular.

A. The search warrant application failed to establish a minimum nexus between the alleged offense and the online accounts

The Fourth Amendment prescribes that “no Warrants shall issue, but upon probable cause.” U.S. Const. amend. IV. To establish probable cause, the issuing judge must have a “substantial basis” for concluding that “a search would uncover evidence of wrongdoing.” *Illinois v. Gates*, 462 U.S. 213, 236 (1983) (quoting *Jones v. United States*, 362 U.S. 257, 271 (1960)). Although the issuing judge is afforded “great deference,” a warrant application cannot rely merely on “conclusory statement[s].” *Id.* at 236, 239 (citing *Nathanson v. United States*, 290 U.S. 41, 54 (1933)).

Whether an affidavit establishes a proper nexus is a fact-intensive question resolved by examining the totality of circumstances presented. See *Gates*, 462 U.S. at 238. “The critical element in a reasonable search is not that the owner of property is suspected of crime, but that there is reasonable cause to believe that the specific ‘things’ to be searched for and seized are located on the property to which entry is sought.” *Zurcher v. Stanford Daily*, 436 U.S. 547, 556 (1978). See, e.g. *United States v. Trivisano*, 724 P.2d 341, 345 (2d Cir. 1983) (“To establish probable cause to search a residence, two factual showings are necessary—first, that a crime was

committed, and second, that there is probable cause to believe that evidence of such crime is located at the residence."); *United States v. Lucan*, 430 F.2d 1051, 1055 (9th Cir. 1970) ("But of course it cannot follow in all cases, simply from the existence of probable cause to believe a suspect guilty, that there is also probable cause to search his residence."); *United States v. Brown*, 828 F.3d 375 (6th Cir. 2016) (Warrant to search defendant's home lacked Fourth Amendment probable cause because warrant affidavit did not state facts directly connecting home with suspected drug dealing activity, defendant's drug dealer status did not give rise for a fair probability that drugs would be found in his home, and there was inadequate evidence of drug dealer status).

The March 14, 2017 warrant to search Mr. Schulte's online accounts is invalid because Donaldson's supporting affidavit did not establish probable cause to believe that evidence of criminal activity *would be found in Mr. Schulte's online accounts*; Donaldson failed to establish a proper nexus between the alleged crime and the online accounts he sought to seize.

1. Probable cause to arrest is not sufficient to conduct a search
Donaldson's affidavit focused entirely upon Mr. Schulte's alleged conduct in March 2016. That information *might* have established probable cause to arrest Mr. Schulte; however, "[t]he warrant application... was for a search warrant, not an arrest warrant. And to obtain a warrant to search for and seize a suspect's possessions or property, the government must do more than show probable cause to arrest him. The government failed to make the requisite showing in this case." *United States v. Griffith*, 867 F.3d 1265, 1271 (D.C. Cir. 2017).

The Supreme Court has long distinguished between arrest warrants and search warrants. See *Stogald v. United States*, 451 U.S. 204, 212-13 (1981). An arrest warrant rests on probable cause to believe that the suspect committed an offense; it thus primarily serves to protect an

individual's liberty interest against an unreasonable seizure of his person. *Id.* at 213. A search warrant, by contrast, is grounded in "probable cause to believe that the legitimate object of a search is located in a particular place." *Id.* Rather than protect an individual's person, a search warrant "safeguards an individual's interest in the privacy of his home and possessions against the unjustified intrusion of the police." *Id.* "The Fourth Amendment's requirements regarding search warrants are not 'formalities.'" *United States v. Voustianlouk*, 685 F.3d 206, 210 (2d Cir. 2012) (quoting *McDonald v. United States*, 335 U.S. 451, 455 (1948)).

In light of the distinctness of the inquiries, probable cause to arrest a person will not itself justify a warrant to search his property. "[A] determination of probable cause to search is not the same as a determination that there is, at the same time, probable cause to arrest, or vice versa." *United States v. Pabon*, 871 F.3d 164, 181 (2d Cir. 2017). In other words, "it cannot follow... simply from the existence of probable cause to believe a suspect guilty, that there is also probable cause to search his residence." *United States v. Valenzuela*, 596 F.2d 824, 828 (9th Cir.), *cert denied*, 441 U.S. 965 (1979). Regardless of whether an individual is validly suspected of committing a crime, an application for a search warrant concerning his property or possessions must demonstrate cause to believe that "evidence is likely to be found at the place to be searched." *Groh v. Ramirez*, 540 U.S. 551, 568 (2004). "There must, of course, be a nexus... between the item to be seized and criminal behavior." *Warden, Md. Penitentiary v. Hayden*, 387 U.S. 294, 307 (1967).

2. The affidavit contained no factual allegations connecting the alleged offenses to Mr. Schulte's online accounts

For a warrant to issue, a magistrate must make a "practical, common-sense decision whether, given all the circumstances set forth in the affidavit... there is a fair probability that

contraband or evidence of a crime will be found in a particular place." *Gates*, 462 U.S. at 238 (1983); See also *United States v. Raymond*, 780 F.3d 105, 113 (2d Cir. 2015). As the text makes clear, "the ultimate touchstone of the Fourth Amendment is 'reasonableness.'" *Brigham City v. Stuart*, 547 U.S. 398, 403 (2006).

a) Google

The search warrant listed two pages of information supposedly tying the alleged crime to the Google account (Ex. A at JAS_118-19). Donaldson discovered that Mr. Schulte used his Google account to "initiate contact, via telephone and text messages, with multiple of his CIA Group colleagues." *Id.* Agent Donaldson believed that since Mr. Schulte used his cellphone to contact former coworkers, with whom he remained friends after he left the CIA, therefore Mr. Schulte must have used his cellphone and Google account to commit espionage. Specifically:

- Mr. Schulte allegedly asked about the status of the investigation, his companion's opinions, and denied involvement.
- Mr. Schulte specifically used his Google account to make some of his inquiries (Donaldson failed to specify anything other than texts/calls).
- On March 7, 2017, when WikiLeaks released the Classified Information, Mr. Schulte sent approximately 149 text messages (Donaldson failed to note this number was statistically equivalent to his average daily texts).
- Mr. Schulte continued to use his Google account after the leak.

Essentially, Donaldson's argument for nexus is the following: (1) Mr. Schulte had a motive and opportunity to take the classified CIA information in March 2016; (2) As of March 2017, Mr. Schulte owns an Android cell phone and therefore has a Google account; (3) Mr. Schulte uses Google's Voice service to send and receive text messages as well as to send and

receive phone calls; therefore, there is probable cause to believe that the Google Account in 2017 contains evidence of espionage committed in 2016.

Is this reasonable? If so, the government need only show that a Target is the owner of an online account, and then they can seize it—for indeed, that is all Donaldson has proven—that Mr. Schulte owned the Google Account, and used one specific service it provided to send and receive text messages. But this fact does not support probable cause that the account contains evidence of a crime—there is literally not a single fact identified linking Mr. Schulte's Google account to any criminal activity. In fact, Agent Donaldson does not even establish when Mr. Schulte created the Google account—or whether it even existed or was used when the Classified Information was stolen from the CIA in March 2016. Furthermore, the Google account was only used because Mr. Schulte had an Android phone and sent/received text messages and phone calls through Google Voice—one specific service offered through Google. Donaldson identified no instances of Mr. Schulte actually using the Google Mail (Gmail) account to send emails or any other Google service aside from Google Voice to send basic text messages and make phone calls like every other person. All Google did was simply send and receive his text messages. But based on this inherently legal activity, Agent Donaldson sought a search warrant to retrieve Mr. Schulte's *ENTIRE* Google account since its inception—including services that Donaldson never mentioned, and which have nothing to do with texting or calling.

b) Reddit

Special Agent Donaldson discovered that on the day of the release of Classified Information by WikiLeaks, the Subject Reddit Account posted "What about this guy pedbsktbl?" followed by a link to Mr. Schulte's GitHub account (Ex. A at JAS_120).

Essentially, Donaldson's argument for nexus is the following: (1) Mr. Schulte had a motive and opportunity to take the classified CIA information in March 2016; (2) In March 2017, a Reddit Account posited that Mr. Schulte could be involved in the CIA leaks; therefore, there is probable cause to believe that the Reddit Account contains evidence of espionage.

Is this reasonable? No, it clearly does not establish probable cause. It does not make any sense that Mr. Schulte would post online pointing blame for the leaks upon himself—Donaldson fails to even establish that Mr. Schulte owned the Reddit account or that it likely contained evidence of espionage. In fact, the Reddit account did not even belong to Mr. Schulte as was discovered after the FBI illegally seized its content.

c) GitHub

Donaldson's search warrant sought the seizure of Mr. Schulte's GitHub account based on the Reddit post mentioned above, and because the GitHub account "contains numerous lines of computer code, some of which reference computer applications that were referenced in the information released by WikiLeaks." (Ex. A at JAS_120-121). That's it. Donaldson failed to mention that these "applications" were Atlassian products that are *publicly* available to anyone. This would be like asking a judge for a search warrant to seize the account because it mentioned "toasters, microwaves, and cookies" and people who worked at the CIA also used them. Absurd.

Essentially, Donaldson's argument for nexus is the following: (1) Mr. Schulte had a motive and opportunity to take the classified CIA information in March 2016; (2) In March 2017, a Reddit Account posited that Mr. Schulte could be involved in the CIA leaks based on content from his GitHub account identifying public applications that were also used at the CIA; therefore, there is probable cause to believe that the GitHub Account contains evidence of espionage.

Is this reasonable? If so, the government can seize any and all online accounts as it need only create a random social media account and post a link to the Target account that they want to search, claiming the owner of the account is guilty. This is absurd; there is clearly no probable cause.

3. Conclusory statements based on "training and experience" do not magically transform an arrest warrant into a search warrant

Special Agent Donaldson explains on page 28 of his affidavit (Ex. A at JAS_121) that probable cause must exist because "Individuals who engage in the Subject Offenses often used Internet-based services (like the Target Accounts) as a means by which to communicate with co-conspirators as well as means through which not only to transmit but also to store purloined information so that they do not have to carry it on their person... I know that WikiLeaks is an Internet-based publication and that individuals who provide information to WikiLeaks in the past oftentimes have done so through the use of other Internet-based computing platforms, like the Target Accounts and other services offered by the Providers."

Conclusory statements such as these do not permit independent probable cause analysis. "Sufficient information must be presented to the magistrate to allow that official to determine probable cause; his action cannot be a mere ratification of the bare conclusions" of others, or an "improper analysis of the totality of the circumstances." *United States v. Leon*, 468 U.S. 897, 915 (1984); *Massachusetts v. Upton*, 466 U.S. 727, 734 (1984); *Gates*, 462 U.S. at 239. Here, the March 14, 2017 warrant application contained no facts connecting the alleged crimes to Mr. Schulte's online accounts. Instead, Agent Donaldson merely offered a conclusory assertion, supposedly based on his "training and experience," that people who steal or disclose classified information tend to use the Internet and online accounts. But this kind of general statement is

precisely the type of "conclusory statement that gives the magistrate virtually no basis at all for making a judgment regarding probable cause." *Gates*, 462 U.S. at 239.

According to Donaldson, he can search any and all of Mr. Schulte's online accounts, homes, cars—literally all of his possessions and every *bit* of data—if he simply establishes that probable cause exists to arrest Mr. Schulte; once established, Donaldson need only interject an "expert statement" based on his "training and experience," and voila—these magic ingredients permit him to search anything his heart desires. If this were all the Fourth Amendment required, it would provide no protection from government intrusion. "The 'basic purpose of this Amendment,' our cases have recognized, 'is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials.'" *Carpenter v. United States*, 138 S. Ct. 2206, 2213 (2017) (quoting *Camara v. Municipal Court of City and County of San Francisco*, 387 U.S. 523, 528 (1967)).

Furthermore, the courts have recognized that a law enforcement officer's purported "expert" opinion about how criminals in general behave is, without more, insufficient to establish probable cause to conduct a search, even where there is probable cause to believe he engaged in a crime. See, e.g., *Griffith*, 867 F.3d at 1274-75 (police officer's opinion, based on his "training and experience," that gang members often use cell phones and other electronic devices to "share intelligence about their activities," did not justify warrant to search suspected gang member's home for such devices in connection with murder investigation). "Indeed, whereas here, there is nothing to connect the illegal activities with the arrested person's apartment, to issue a warrant based solely on the agent's expert opinion would be to license virtually automatic searches of residences of persons arrested for narcotics offenses. This would effectively eviscerate the fourth amendment's requirement that there be probable cause to believe 'that

contraband or evidence of a crime will be found in a particular place.” *United States v. Gomez*, 652 F. Supp. 461, 463 (E.D.N.Y. 1987) (quoting *Gates*, 462 U.S. at 238); *United States v. Schultz*, 14 F.3d 1093, 1097 (6th Cir. 1994) (an officer’s training and experience “cannot substitute for the lack of evidentiary nexus”); *United States v. Roman*, 942 F.3d 43 (1st Cir. 2019) (Training and experience and other conclusory statements from law enforcement are insufficient to establish probable cause without “specific observations”); *United States v. Christian*, 893 F.3d 846 (6th Cir. 2018) (same); *United States v. Guzman*, No. 97 Cr. 786 (SAS), 1998 WL 61850, at *2 (S.D.N.Y. Feb. 13, 1998) (finding no probable cause even when the affidavit included “general averments based on [the affiant’s] training and experience”); *United States v. Rios*, 881 F. Supp. 772, 775-76 (D. Conn. 1995) (same).

Finally, while Agent Donaldson’s averment about individuals who engage in drug trafficking or other typical crimes may be accurate, there are almost no cases of espionage—particularly espionage related to the theft of digital data. From what “experience” does Donaldson derive his knowledge? Has Donaldson ever worked an espionage case involving the alleged theft of digital files from the CIA? Has he ever worked an espionage case involving digital files? Has he ever worked on an espionage case *at all*? What espionage cases have even been brought against defendants living in New York City or in the Second Circuit’s realm—particularly during Donaldson’s employment? Based on all criminal complaints, indictments, and other public information, there was not a single espionage case in the Second Circuit during Donaldson’s employment from 2010 to present. Donaldson’s conclusory statements purportedly based on his “experience” are nothing but a fabrication—Agent Donaldson has no experience investigating espionage cases, nor sufficient experience to indicate the likelihood or probability that criminal activity will exist on Mr. Schulte’s online accounts. And what “training” does

Donaldson refer? Does the FBI offer a class where it "trains" all its agents to suspect that anyone accused of any crime may leave evidence of their crime at any place and on any electronics, so its agents can claim "training and experience" in every warrant for any case? It's absolutely absurd to believe the government can execute a search and seizure warrant simply because the government says the magic words "training and experience." This boilerplate magic does not bypass the Fourth Amendment—the government cannot execute a search simply because it wants.

4. The allegations concerning the theft of national defense information in March 2016 were too stale to justify searching Mr. Schulte's online accounts a full year later in March 2017.

Special Agent Donaldson alleged in his affidavit that Mr. Schulte stole the national defense information in March of 2016. Yet, Donaldson failed not only to establish any link at all between the theft and Mr. Schulte's online accounts, but he also failed to establish that the online accounts existed in 2016. Since probable cause must "exist as of the time of the search and not simply as of some time in the past, the facts in an affidavit supporting a search warrant must be sufficiently close in time to the issuance of the warrant and the subsequent search conducted." *United States v. Wagner*, 989 F.2d 69, 75 (2d Cir. 1993); see also *United States v. Grubbs*, 547 U.S. 90, 95 n.2 (2006). "The two critical factors in determining staleness are the age of the facts alleged and the nature of the conduct alleged to have violated the law." *Raymond*, 780 F.3d at 114 (internal quotation marks omitted). Additional relevant factors include the nature of the information forming the basis for probable cause, and the nature of the evidence being sought. *United States v. McGrath*, 622 F.2d 36, 41-42 (2d Cir. 1980).

Here, the relevant factual allegations were too stale to establish probable cause to search Mr. Schulte's online accounts on March 14, 2017. The allegations in the warrant detailed a theft

one year earlier in 2016—it merely established probable cause that the “facts support a conclusion that Schulte had both a motive and opportunity to take the classified CIA information,” but detailed nothing about transmission of the information or WikiLeaks itself; there is no indication, speculation, or theory of what happened to the information after March 2016. Therefore, Donaldson must at the very least establish that Mr. Schulte possessed the same online accounts in 2016—how could incriminating evidence exist on the accounts if they were not created until *after* the information was stolen? Donaldson’s only information about the accounts is they existed as of March 7, 2017. Hence, not only does Donaldson fail to link the alleged criminal activity to the online accounts, but he fails to establish that the online accounts even existed when the crime occurred!

Additionally, the stateness provided an *entire year* during which all evidence of the alleged crime could easily be completely destroyed. As the affidavit acknowledged, Mr. Schulte possessed “a skill set that enabled him to write computer code” to perform “clandestine[]” operations (Ex. A at JAS_110, 18(a)(iii)); Mr. Schulte was a malware developer trained by the CIA to conduct cyber operations against foreign adversaries. Why wouldn’t Mr. Schulte immediately transfer and delete the data? The nature of the crime is completely unlike typical drug or child pornography offenses that require consistent possession of the contraband itself—alternatively, espionage offenses generally encourage rapid transmission and instant deletion of the contraband; there’s absolutely no logical or legitimate reason to keep such information for any duration, let alone an entire year.

In light of the nature of the crime and typical criminal, ample opportunity to delete incriminating evidence, sophistication of the crime, incentive to rapidly transfer and delete any incriminating evidence, and Mr. Schulte’s expertise for covert operations from the CIA, it is

highly unlikely any evidence of criminal activity would be found on the online accounts. See *Griffith*, 867 F.3d at 1275 (recognizing that “the opportunities those involved in crime would have had to remove or destroy [incriminating] items’ ... is an important consideration, when assessing the existence of probable cause”) (quoting 2 Wayne R. LaFare, *Search and Seizure* § 3.7(a) (5th ed. 2016)); see also *United States v. Paul*, 692 F. Supp. 186, 193 (S.D.N.Y. 1988) (holding that based on the isolated nature of the alleged extortion, “it is more reasonable to infer that an extortionist would seek to disperse or spend his booty in an attempt to hide it”; thus, information in affidavit was too stale to establish probable cause).

5. Given the totality of the circumstances, Donaldson’s warrant failed to establish the necessary nexus between the alleged crime and Mr. Schulte’s online accounts

“(I)t is generally understood that ‘probable cause to search is determined where the totality of the circumstances indicates a fair probability that contraband or evidence of a crime will be found at a particular place.’” *United States v. Clark*, 638 F.3d 89, 93 (2d Cir. 2011) (quoting *Walczyk v. Rja*, 496 F.3d 139, 156 (2d Cir. 2007)). Probable cause to search must be based on a “sufficient nexus between the criminal activity alleged” and the location or items to be searched. *United States v. Singh*, 390 F.3d 168, 182 (2d Cir. 2004). See, e.g., *United States v. Rivera*, 825 F.3d 59, 66 (1st Cir. 2016) (probable cause where the evidence “indicated that [defendant] participated in a drug-related phone call from his home”).

Given the “totality of the circumstances,” Donaldson’s supporting affidavit failed to establish a “sufficient nexus between” the alleged crimes of espionage and the online accounts to search, and therefore failed to establish “a fair probability that contraband or evidence of a crime” would be found on the online accounts. Even assuming Donaldson’s warrant established probable cause to believe Mr. Schulte committed a crime, it came nowhere close to establishing

probable cause to believe that evidence of the crime would exist on the Target accounts; the warrant identified only that Mr. Schulte owned (some) of the online accounts, but failed to establish anything except nonnet-use, legal activity on the inherently legal online accounts; Donaldson sought to cure the facially deficient affidavit with "magic" generic, conclusory statements based on his "training and experience" that courts have firmly warned does not cure the facial deficiency and which the statements themselves are doubtful as Donaldson has likely never worked on a similar case and has no "experience" with which to relate and any "training" is not based on real-world examples; and finally, the warrant not only failed to link the online accounts to any crime, but also failed to establish that the online accounts even existed during the timeframe the alleged crime occurred.

In summary, given (1) no factual basis linking Mr. Schulte's online accounts to the alleged theft in 2016 and (2) no establishment that the online accounts even existed in 2016, the affidavit provided no factual basis to conclude incriminating evidence would be found on Mr. Schulte's online accounts in 2017. Additionally, considering (3) Donaldson's conclusory statements about "training and experience" are patently false, (4) the year-long period between the alleged theft of the national defense information (March 2016) and the application for the search warrant (March 2017), (5) Mr. Schulte's acknowledged expertise in computers and covert operations, and (6) no incentive to retain the national defense information after transfer, it is almost a certainty that, even if Mr. Schulte were guilty, his online accounts in 2017 would contain absolutely no evidence of the alleged crime. Nor did the government find any such evidence after its unconstitutional search. Finding the existence of probable cause in this case would verge on authorizing a search warrant anytime there is probable cause to suspect someone of a crime—which would "effectively eviscerate the fourth amendment."

Accordingly, Donaldson's search warrant affidavit fails to establish this requisite nexus and therefore the warrant is invalid under the Fourth Amendment. See, e.g., *United States v. Brown*, 828 F.3d at 382 ("the search warrant affidavit contained no evidence that [the defendant] distributed narcotics from his home, that he used it to store narcotics, or that any suspicious activity had taken place there"); *United States v. Buln*, 874 F.3d 1, 23-24 (1st Cir. 2017) ("We have expressed skepticism that probable cause [to search a home] can be established by the combination of the fact that defendant sells drugs and general information from police officers that drug dealers tend to store evidence in their homes. However, the addition of specific facts connecting the drug dealing to the home can establish a nexus.") (Internal citations omitted), cert. denied, 138 S. Cl. 1593 (2018); *United States v. Benevento*, 836 F.2d 60, 70 (2d Cir. 1987) (Expressing skepticism that probable cause to search home can be established by expert's conclusory statements standing alone, but rather, establishing probable cause upon "specific statements from the government's confidential informants that provided key details of various aspects of the narcotics conspiracy"); *United States v. Lahey*, 967 F. Supp. 2d 698, 712 n. 16 (S.D.N.Y. 2013) ("But the question of whether there was probable cause to believe that [the defendant] was a drug dealer is potentially distinct from the question of whether there was probable cause to search his apartment"); *Kortright*, 2011 WL 4406352 at *7 (finding no probable cause where "the only factual link in the Affidavit between Defendant's alleged criminal activity and the Apartment is the fact that Defendant resided at the Apartment"); *United States v. Moran*, 349 F. Supp. 2d 425, 476 (N.D.N.Y. 2005) ("[M]ore residence by a suspect does not constitute a fair probability that evidence of the criminal activity will be found there."); See also *Griffith*, 867 F.3d at 1273 ("To justify a search of the apartment... police needed reason to think not only that [defendant] possessed a phone, but also that the device would be located in

the home and would contain incriminating evidence about his suspected offense.”); *Roman*, 942 F.3d at 54 (The affidavit failed to establish “a clear and substantial connection between the illegal activity and the place searched; rather, the government’s argument relies upon speculative inferences piled upon inferences”).

B. The search warrant application was insufficiently particular, overbroad, and authorized a general warrant

The lack of probable cause to search Mr. Schulte’s online accounts itself renders the warrant invalid under the Fourth Amendment. But the warrant was also invalid for an additional reason: its lack of particularity to each category of digital information it sought to seize and its overbreadth, unjustified by the probable cause upon which the warrant was based, unlimited in scope, and not narrowly tailored as required by law, purported to authorize a general warrant—the very instrument for which the Fourth Amendment was ratified to prohibit.

“The chief evil that prompted the framing and adoption of the Fourth Amendment was the ‘indiscriminate searches and seizures’ conducted by the British ‘under the authority of general warrants.’” *United States v. Galpin*, 720 F.3d 436, 445 (2d Cir. 2013) (quoting *Payton v. New York*, 445 U.S. 573, 583 (1980)); *Arizona v. Grant*, 556 U.S. 332, 345 (2009) (“[T]he central concern underlying the Fourth Amendment [is] the concern about giving police officers unbridled discretion to rummage at will among a person’s private effects.”). “[T]he Fourth Amendment’s proscription of unreasonable searches and seizures ‘not only... prevent[s] searches and seizures that would be unreasonable if conducted at all, but also... ensure[s] reasonableness in the manner and scope of searches and seizures that are carried out.’” *Laurio v. Charles*, 219 F.3d 202, 209 (2d Cir. 2000) (quoting *Ayeni v. Mottola*, 35 F.3d 680, 684 (2d Cir. 1994)).

1. Agent Donaldson sought a general warrant to seize Mr. Schulte's entire electronic footprint since birth

a) Google

See Ex. A at JAS_128-131: Search History, Google+ Photos and Content, Google Drive Content, Google Voice, Google Wallet Content, Youtube Content, Android Content, Email Content, Address Book Information, Subscriber and Payment Information, Linked Accounts, Transactional Records, Customer Correspondence, Preserved Records.

b) Reddit

See Ex. A at JAS_134-136: Search History, Post Content, Email Content or Direct Message Content, Subscriber and Payment Information, Transactional Records, Customer Correspondence, Preserved Records.

c) GitHub

See Ex. A at JAS_139-141: Use of GitHub Features, GitHub Platforms, GitHub Repositories, Email Content or Direct Message Content, Address Book Information, Subscriber and Payment Information, Transactional Records, Customer Correspondence, Preserved Records.

2. The special privacy concerns that apply to the search of personal electronic data and the particularity requirement

Special Agent Donaldson sought to seize, search, and examine virtually every aspect of Mr. Schulte's personal life. Digital searches "demand[] a heightened sensitivity to the particularity requirement" because of the "serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant." *Galpin*, 720 F.3d at 447 (quoting *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1176 (9th Cir. 2010) (quotation marks omitted)). "The sheer volume of data that

may be stored on an electronic device [or cloud-based storage] raises a significant likelihood that much of the data on the device that has been seized will be deeply personal and have nothing to do with the investigation of criminal activity. For this reason, we have recognized the special concerns that apply when law enforcement seize and search people's personal electronic data and communication devices." *United States v. Smith*, 967 F.3d 198, 207 (2d Cir. 2020). "Tax records, diaries, personal photographs, electronic books, electronic media, media data, records of internet searches, banking and shopping information—all may be kept in the same device, interspersed among the evidentiary material that justifies the seizure or search." *Id.* (quoting *United States v. Garlas*, 824 F.3d 199, 218 (2d Cir. 2016) (en banc)). "The upshot is that the search and seizure of personal electronic devices like a modern cell phone or tablet computer implicates different privacy and possessory concerns than the search and seizure of a person's ordinary personal effects." *Id.* at 208.

Although the search here was not to seize a cellphone, Mr. Schulte's Google Account stored all of the data from his android cellphone and then some. "[T]he data a user views on many modern cell phones may not in fact be stored on the device itself... That is what cell phones, with increasing frequency, are designed to do by taking advantage of cloud computing. Cloud computing is the capacity of Internet-connected devices to display data stored on remote servers rather than on the device itself... Moreover, the same type of data may be stored locally on the device for one user and in the cloud for another." *Riley v. California*, 573 U.S. 373, 394, 397 (2014). Hence, the analysis in *Riley* is pertinent for a seizure and search of the same data that is stored on the "cloud."

a) The search for digital information and the associated privacy concerns, as explained in Riley v. California

In *Riley*, the Supreme Court held that the police generally may not, without a warrant, search digital information on a cell phone seized from an individual who has been arrested. The Court's opinion in *Riley* went to great lengths to explain the range of possible types of information contained on cellphones, and the associated privacy concerns inherent in searches of digital information.

The *Riley* Court explained that cell phones "are in fact minicomputers that also happen to have the capacity to be used as a telephone" as well as "*cameras, video players, rolodexes, calendars, tape recorder, libraries, diaries, albums, televisions, maps, or newspapers.*" *Id.* at 393 (emphasis added). It distinguished "modern cell phones in their immense storage capacity" that may contain "every piece of mail [people] have received for the past several months, every picture they have taken or every book or article they have read... *photographs, picture messages, text messages, Internet browsing history, a calendar, a thousand-entry phone book, and so on.*" *Id.* at 394-95 (emphasis added).

"The storage capacity of cell phones has several interrelated consequences for privacy. First, a cell phone collects in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that *reveal much more in combination than any isolated record.* Second, a cell phone's capacity allows even just one type of information to convey far more than previously possible. The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions... Third, the data on a phone can date back to the purchase of the phone, or even earlier." *Id.* at 394-95 (emphasis added).

"Although the data stored on a cell phone is distinguished from physical records by quantity alone, certain types of data are also qualitatively different. An *Internet search and browsing history*, for example, can be found on an Internet-enabled phone and could reveal an individual's private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD. Data on a cell phone can also reveal where a person has been. Historical location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building." *Id.* at 395-96.

"Mobile application software on a cell phone, or 'apps,' offer a range of tools for managing detailed information about all aspects of a person's life. There are apps for Democratic Party news and Republican Party news; apps for alcohol, drug, and gambling addictions; apps for sharing prayer requests; apps for tracking pregnancy symptoms; apps for planning your budget; apps for every conceivable hobby or pastime; apps for improving your romantic life. There are popular apps for buying or selling just about anything, and the records of such transactions may be accessible on the phone indefinitely. There are over a million apps available in each of the two major app stores... The average smart phone user has installed 33 apps, which together can form a revealing montage of the user's life." *Id.* at 396.

"Indeed, a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is." *Id.* at 396-97.

In summary, the Court concluded that “[m]odern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans ‘the privacies of life.’ The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought.” *Id.* at 403 (internal quotation omitted, emphasis added).

b) Riley requires probable cause to search each category of digital information

The Google account contained even more data than the Android cell phone; it essentially amounted to a computer hard drive, containing search history, files, photos, videos, emails, etc. “Where, as here, the property to be searched is a computer hard drive, the particularity requirement assumes even greater importance. As numerous courts and commentators have observed, advances in technology and the centrality of computers in the lives of average people have rendered the computer hard drive akin to a residence in terms of the scope and quantity of private information it may contain.” *Galpin*, 720 F.3d at 446.

All of this incredibly private, personal data—information the Supreme Court has forbidden Donaldson to seize from an arrest warrant. Donaldson, who was chomping at the bit to get ahold of this extremely sensitive data, simply gave the Supreme Court a run around, and went straight to the source of the data itself, Google, to obtain a general warrant to obtain ALL this incredibly sensitive, private, and protected data based on literally *nothing*. See Jim Kerstetter, *Microsoft Goes on Offensive Against Justice Department*, N.Y. Times (Apr. 15, 2016) (“When customer information is stored in a giant data center run by companies like Google, Apple, and Microsoft, investigators can go straight to the information they need, even getting a judge to order the company to keep quiet about it.”). Each and every service Google offers, and

each and every type of information Google provides, *should have been subject to its own requirement of probable cause*; just because Mr. Schulte chose to use Google to manage all of his content should not mean that the Fourth Amendment does not protect that data. See *United States v. Morton*, 984 F.3d 421, 425-26 (5th Cir. 2021) (“*Riley* made clear that these distinct types of information, often stored in different components of the phone, should be analyzed separately. This requirement is imposed because ‘a cell phone’s capacity allows even just one type of information to convey far more than previously possible.’ ... In short, *Riley* rejected the premise that permitting a search of all content on a cellphone is ‘materially indistinguishable’ from other types of searches. Absent unusual circumstances, probable cause is required to search *each category of content*.” (quoting *Riley*, 573 U.S. at 393-395)).

If Mr. Schulte used different and unique providers for search, photos, data storage, videos, contents, email—could Donaldson obtain warrants to seize each and every provider based on Mr. Schulte’s use of a single provider? No, this would be absurd; If Mr. Schulte had an iPhone and sent text messages through Apple, it would surely be absurd for Donaldson to apply for a search warrant to Yahoo to seize all his emails, to Facebook to seize all of his photos, to Dropbox to receive all of his files, to Paypal to seize all financial information, to Microsoft to seize all of his search history, and to Fitbit to seize all GPS data—all because Mr. Schulte used Apple to send text messages? Surely, the magistrate would laugh Donaldson out on his ass. Yet, because Google offers all services, it somehow becomes permissible for Donaldson to do just that? Donaldson’s warrant failed to identify probable cause for each type of information it sought to seize; it was a general, exploratory rummaging in Mr. Schulte’s private digital data—incontrovertibly unconstitutional.

3. The Donaldson warrant was insufficiently particular as it was broader than justifiable by the probable cause upon which the warrant was based

To prevent "general, exploratory rummaging in a person's belongings" and the attendant privacy violations, *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971), the Fourth Amendment provides that "a warrant may not be issued unless probable cause is properly established and the scope of the authorized search is set out with particularity," *Kentucky v. King*, 561 U.S. 452 (2011). "The manifest purpose of this particularity requirement was to prevent general searches. By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement ensures that the search will be carefully tailored to its justification and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit." *Maryland v. Garrison*, 480 U.S. 79, 84 (1987). "A failure to describe the items to be seized with as much particularity as the circumstances reasonably allow offends the Fourth Amendment because there is no assurance that the permitted invasion of a suspect's privacy and property are no more than absolutely necessary." *United States v. George*, 975 F.2d 72, 76 (2d Cir. 1992). Consequently, a warrant with an "indiscriminate sweep" is "constitutionally intolerable." *Stanford v. Texas*, 379 U.S. 476, 478 (1965).

"To satisfy the Fourth Amendment's particularity requirement, a warrant must meet three criteria: (1) it 'must identify the specific offense for which the police have established probable cause'; (2) describes the place to be searched; and, (3) it 'must specify the items to be seized by their relation to designated crimes.'" *United States v. Purcell*, 967 F.3d 159, 178 (2d Cir. 2020) (quoting *Galpin*, 720 F.3d at 445-46). "A warrant is facially unconstitutional if it fails to comply with any of these three requirements." *Id.*

Donaldson's affidavit failed on the second and third requirements. In obligating officers to describe the items to be seized with particularity, the Fourth Amendment prevents "the issu[ance] of warrants on loose, vague or doubtful bases of fact." *Go-Bart Importing Co. v. United States*, 282 U.S. 344, 357 (1931). In that way, the particularity requirement "is necessarily tied to the... probable cause requirement." *In re 650 Fifth Ave. & Related Props.*, 830 F.3d 66, 99 (2d Cir. 2016). See *United States v. Buck*, 813 F.2d 588, 590-592 (2d Cir. 1987) (finding that a warrant authorizing the seizure of "any papers, things, or property of any kind relating to [the] previously described crime" failed the particularization requirement because it "only described the crimes—and gave no limitation whatsoever on the kind of evidence sought."). "An otherwise unobjectionable description of the object to be seized is defective if it is broader than can be justified by 'the probable cause upon which the warrant is based.'" *Galpin*, 720 F.3d, at 446 (quoting 2 Wayne R. LaFare, *Search and Seizure* § 4.6(a) (5th ed. 2012)).

How did Donaldson "specify the items to be seized by their relation to designated crimes?" How is the seizure of each category of data *justified by the probable cause upon which the warrant is based*? What probable cause justifies the seizure of photos when the warrant fails to mention anything about photos? And how can photos possibly contain evidence of the alleged crime? Videos? Purchase history? Address book and all contacts? Transactional records? Linked accounts? Cell phone content? Search history? Post content? Digital files? "There must be a specific factual basis in the affidavit that connects each cellphone feature to be searched to the [alleged] crimes." *Morton*, 984 F.3d at 427. In fact, what limitations exist for the scope of the warrant? Is there any limitation at all? Is there any scope at all? Is there any data Donaldson's warrant does not seize?

Here, the search was unlimited in scope without justification, and therefore unconstitutional. Indeed, Donaldson's warrant literally sought the seizure of all documents from all accounts. Instead of requesting a search of "EVERYTHING" which he knew would be unconstitutional, Donaldson thought it clever to simply *enumerate* EVERYTHING without actually saying "EVERYTHING"—alas, the result is the same—a warrant that purports to authorize the seizure of, literally, all documents. A warrant that purports to "authorize the seizure of, essentially, all documents" exceeds the scope of probable cause. *United States v. Wey*, 256 F. Supp. 3d 355, 393 (S.D.N.Y. 2017). Here, just as in *Wey*, the warrant lacked particularly where it set forth "expansive categories of often generic items subject to seizure—several of a 'catch-all' variety—without, crucially, any linkage to the suspected criminal activity" *Id.* at 385; without a more limited scope of what types of documents to search, and their *relation* to the alleged crime, the search is not narrowly tailored and particularity fails. See *United States v. Burgess*, 576 F.3d 1078, 1091 (10th Cir. 2009) ("If the warrant is read to allow a search of all computer records without description or limitation it would not meet the Fourth Amendment's particularity requirement."); *United States v. Reilly*, 76 F.3d 1271, 1273 (2d Cir. 1996) ("A warrant is not a general hunting license..."). Yet, this was Donaldson's goal—to obtain a general hunting license and rummage through every single document without establishing probable cause for such a wide scope. Donaldson's affidavit essentially states "Mr. Schulte may possess some classified information—*because I say so*—so permit me to rummage through *all* his documents until I find something I can use against him in a criminal prosecution."

Donaldson's overbroad warrant is precisely the type of general warrant feared by America's founding fathers: "Our cases have recognized that the Fourth Amendment was the founding generation's response to the reviled 'general warrants' and 'writs of assistance' of the

colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity" and that "opposition to such searches was in fact one of the driving forces behind the Revolution itself." *Riley*, 573 U.S. at 403; *Stanford v. Texas*, 379 U.S. at 486 ("[T]he Fourth... Amendment [] guarantee[s]... that no official... shall ransack [a person's] home and seize his books and papers under the unbridled authority of a general warrant...").

Altogether, the warrants to search ALL electronic data on Google, Reddit, and GitHub "lacked the requisite specificity to allow for a tailored search of [the defendant's] electronic media" and "fail[ed] to link the items to be searched and seized to the suspected criminal activity." *United States v. Rosa*, 626 F.3d 56, 62 (2d Cir. 2010). It is incontrovertible that Donaldson's search warrant violated the Fourth Amendment to the United States Constitution.

C. The good-faith exception to the exclusionary rule does not apply

The invalidity of a search warrant does not always require suppressing evidence recovered in its execution. Under the good-faith exception to the exclusionary rule, "evidence seized in reasonable, good-faith reliance on a search warrant" need not be excluded, even if the warrant turns out to have been unsupported by probable cause. *Leon*, 468 U.S. at 905 (citation omitted).

"The exclusionary rule serves to deter deliberate, reckless, or grossly negligent [police] conduct." *Herring v. United States*, 555 U.S. 135, 144 (2009). However, the application of the exclusionary rule and suppression of evidence do not require a showing of bad faith in relying on an invalid warrant. See *Groh*, 540 U.S. at 563-65 & n.8. Evidence obtained pursuant to a warrant should be excluded in any of the following circumstances: "(1) where the issuing magistrate has been knowingly misled; (2) where the issuing magistrate wholly abandoned his or her judicial

role; (3) where the application is so lacking in indicia of probable cause as to render reliance upon it unreasonable; (4) where the warrant is so factually deficient that reliance upon it is unreasonable." *United States v. Moore*, 968 F.2d 216, 222 (2d Cir. 1992) (citing *Leon*, 468 U.S. at 923).

The good-faith exception fails in this case due to the third and fourth reason: the warrant application was so lacking in indicia of probable cause, and the face of the warrant was so plainly overbroad, no reasonably well-trained officer could have possibly believed it to be valid. This failure "most often applies 'when affidavits are bare bones, i.e., totally devoid of factual circumstances to support conclusory allegations.'" *United States v. Rissaw*, 580 Fed. Appx. 35, 36 (2d Cir. 2014) (quoting *Clark*, 638 F.3d at 103).

The classic bare-bones affidavit asserts only an officer's conclusion that probable cause exists "without any statement of adequate supporting facts." *Nathanson v. United States*, 290 U.S. at 46. For search warrants, this test is met when the affidavit lacked any allegation tying illegal activity to the place to be searched, *Brown*, 828 F.3d at 385-86; *United States v. McPhearson*, 469 F.3d 518, 526-27 (6th Cir. 2006), or when it contained no basis to believe that contraband would still remain there. An affidavit seeking a search warrant is not bare bones, by contrast, if it contains "some modicum of evidence, however slight, between the criminal activity at issue and the place to be searched[.]" *United States v. White*, 874 F.3d 490, 497 (6th Cir. 2017) (citation omitted).

When applying that standard, courts consider the objective reasonableness not only of "the officers who eventually executed the warrant, but also of the officers who originally obtained it or who provided information material to the probable-cause determination." *Leon*,

468 U.S. at 923 n.24. The question is whether an objectively reasonable officer could believe in good faith that the affidavit established probable cause, keeping in mind the inadequacy of a "bare bones" affidavit. *Id.*

Since a search warrant requires not only probable cause to believe that a crime has been committed, but also a nexus between the alleged crime and the place to be searched and things to be seized, the good faith exception does not apply where the warrant application contains no facts to establish even a minimal nexus, because no law enforcement officer could "reasonably believe that the warrant was based on a valid application of the law to the known facts." *Reilly*, 76 F.3d at 1280. See, e.g., *Griffith*, 867 F.3d at 1278 (good-faith exception inapplicable where warrant application alleged no factual nexus to home and improperly sought permission "to search for and seize any electronic device found in the home"); *United States v. Gonzales*, 399 F.3d 1225, 1231 (10th Cir. 2005) (exception inapplicable where affidavit alleged no facts showing even a "minimal nexus between the place to be searched and the suspected criminal activity;" detective merely stated that, in his general experience, "firearm[s] are often kept at the residence").

Here, conclusory assertions aside, the affidavit provided no facts connecting Mr. Schulte's online accounts to the offenses—no factual basis for assuming that any incriminating evidence would be found there in March 2017. Instead, the affidavit contained a single conclusory paragraph purporting to establish probable cause based solely on "training and experience" without establishing a single fact even remotely linking the alleged crime to the online accounts—a "bare bones" affidavit. "The good faith exception does not apply to bare bones affidavit based entirely on unsubstantiated conclusions." *Clark*, 638 F.3d at 103 (citation omitted). See *United States v. Wilhelm*, 80 F.3d 116, 121 (4th Cir. 1996) (A "bare bones"

affidavit is one that contains "wholly conclusory statements, which lack the facts and circumstances from which a magistrate can independently determine probable cause." (quoting *United States v. Laury*, 985 F.2d 1293, 1311 n.23 (5th Cir. 1993)); *McPherson*, 469 F.3d 518 (it is objectively unreasonable to issue a search warrant based upon a "bare bones affidavit... that merely 'states suspicions, beliefs, or conclusions, without providing some underlying factual circumstances regarding veracity, reliability, and basis of knowledge.'"); *Roman*, 942 F.3d 43 (same).

Additionally, since Donaldson's warrant violated the Fourth Amendment by failing to particularize the data to seize relative to the established probable cause, the warrant swept too broadly and no reasonably well-trained agent could have possibly believed it to be valid. Wholesale suppression is required when government agents "(1)... effect a widespread seizure of the items that were not within the scope of the warrant and (2) do not act in good faith." *United States v. Shi Yan Liu*, 239 F.3d 138, 140 (2d Cir. 2000) (citations and internal quotation marks omitted); See also *United States v. Reilly*, 589 F.2d 418, 423 (9th Cir. 1978) (ordering blanket suppression where, "as interpreted and executed by the [searching] agents, the warrant became an instrument for conducting a general search"). See *United States v. Leary*, 846 F.2d 592, 606-610 (10th Cir. 1988) (declining to apply the good-faith exception where the warrant swept too broadly in describing the items subject to seizure and search).

"Good faith is not a magic lamp for police officers to rub whenever they find themselves in trouble," *United States v. Reilly*, 76 F.3d at 1280. The "sole purpose" of the exclusionary rule "is to deter future Fourth Amendment violations." *Davis v. United States*, 564 U.S. 229, 236-37 (2011). Agent Donaldson's search warrant here is precisely the type of warrant that the exclusionary rule sought to discourage—the deliberate pillaging of Mr. Schulte's property and

total evisceration of the Constitution's Fourth Amendment guarantee through malicious police misconduct and abuse; Donaldson sought a general warrant cloaking him in the King's power to do no wrong—his actions are no different from those that incited the first Americans to rise up and overthrow the fascist British Crown. To condone Agent Donaldson's actions would be to undermine everything that revolution stood for, and would be a complete repudiation of the Constitution and renunciation of the Fourth Amendment. Taken together, those failings as to probable cause, particularity, and overbreadth bring the warrant well beyond the good-faith exception's reach.

III. MOTION FOR SEVERANCE / BIFURCATION

A. The MCC counts are improperly joined with the WikiLeaks counts and should be severed

The Third Superseding Indictment charges Mr. Schulte with two distinct acts of offenses:

(1) the alleged theft from the CIA and transmission of classified information to WikiLeaks ("WikiLeaks counts") and (2) the alleged "attempted" disclosure of already public information ("MCC counts"); the MCC counts and WikiLeaks counts are not similar in character, based on the same act, or connected by any common scheme, and they should therefore not be tried together in a single trial.

Separate offenses may be charged in the same indictment only if they are (1) "of the same or similar character"; (2) "based on the same act or transaction"; or (3) "connected with or constitute parts of a common scheme or plan." Fed. R. Crim. P. 8(a). "Similar charges" include those that are "somewhat alike," "resembling in many respects," or those "having a general likeness," to each other. *United States v. Werner*, 620 F.2d 922, 926 (2d Cir. 1980) (quotation omitted). "Joinder is usually proper... when counts 'have a sufficiently logical connection to

each other' or 'where the same evidence may be used to prove each count.'" *United States v. Ezeobi*, No. 10 CR. 669 DLC, 2011 WL 3625662, at *1 (S.D.N.Y. Aug. 17, 2011) (quoting *United States v. Rivera*, 546 F.3d 245, 253 (2d Cir. 2008)). "In reviewing the propriety of joinder, courts 'apply a commonsense rule to decide whether, in light of the factual overlap among charges, joint proceedings would produce sufficient efficiencies such that joinder is proper notwithstanding the possibility of prejudice to... the defendant[] resulting from the joinder.'" *United States v. Kerk*, 615 F. Supp. 2d 256, 274 (S.D.N.Y. 2009) (quoting *United States v. Shellaf*, 507 F.3d 82, 98 (2d Cir. 2007)).

Here, there is no factual overlap between the MCC counts and WikiLeaks counts, and few efficiencies to a joint trial because the evidence on the MCC counts is substantially different from the evidence on the WikiLeaks counts. The government's anticipated evidence on the WikiLeaks counts is almost non-existent, the bulk of which includes testimony and evidence with no bearing on the actual crime, but rather simply to establish motive. The crime was allegedly committed in Virginia of 2016 when Mr. Schulte worked at the CIA and had access to classified information. The circumstantial evidence and the government's theory is extremely complex and confusing, somehow claiming Mr. Schulte stole information from the CIA without ever accessing the virtual machine from which the data was stored, without connecting any removable media to extract the data, and then transmitted it to WikiLeaks without ever contacting WikiLeaks or even visiting its website. In contrast, the MCC counts were allegedly committed in a New York City prison two and a half years later, and mostly involve the "attempted" disclosure of information already publicly accessible from the Internet. These allegations are vastly dissimilar, with literally no overlap.

First, there is no allegation that the MCC counts are based on the same act or transaction as the WikiLeaks counts. *See Shellaf*, 507 F.3d at 100 (joinder of non-tax counts with tax count improper because the non tax counts “neither depended upon nor necessarily led to the commission of the alleged... tax misconduct and proof of the one act neither constituted nor depended upon proof of the other”). The MCC counts are exclusively based on conduct occurring after September 2018, while Mr. Schulte was at the MCC in New York. In contrast, the WikiLeaks counts are based on alleged conduct occurring around April 2016, while Mr. Schulte worked at the CIA in Virginia, and before Mr. Schulte was arrested or charged with any crimes.

It also cannot be said that the MCC charges are part of a common scheme or plan as the WikiLeaks charges. There is no allegation that the MCC charges arose out of the WikiLeaks-related conduct, nor that the WikiLeaks offenses led to the MCC counts. Moreover, like the child pornography counts, the MCC counts were allegedly committed during a completely different time period and from a different place than the WikiLeaks counts. *See, e.g., United States v. Martinez*, 92-CR-839(SWK), 1993 WL 322768, at *9 (S.D.N.Y. Aug. 19, 1993) (“[T]he superseding indictment in no way suggests that the possession of the weapon... has any relation to the narcotics conspiracy” in part because “[t]he gun was seized over four months later, at a completely different location, under circumstances having no bearing on... the alleged narcotics conspiracy”); *Shellaf*, 507 F.3d at 88 (reversing denial of motion to sever tax count from non-tax counts where tax violation occurred “before the conspiracy and wire fraud allegedly began”). Critically, the context and purpose of Mr. Schulte’s alleged conduct at the MCC—to share information from the Internet—differs sharply from the presumed objective of the WikiLeaks counts. *See United States v. Oaks*, 285 F.Supp.3d 876, 880 (D. Md. 2018) (finding no common

scheme between the obstruction of justice count and wire fraud counts because the defendant's "scheme to commit bribery and his scheme to obstruct justice are two distinct efforts that lack a shared objective"). In short, there is nothing to indicate that the MCC counts and WikiLeaks counts are parts of a common plan or scheme.

Additionally, Mr. Schulte's defense is substantially different in both cases. While Mr. Schulte commit neither crime, he will principally argue in the MCC counts that it does not matter even if he did the alleged acts, because his actions are protected by the First Amendment right to free speech—the government cannot indict and prosecute people for republishing information already on the internet. No jury could possibly convict, because, as Mr. Schulte will argue at trial—how would they like to be indicted, tortured in solitary confinement indefinitely, and hauled into trial because they retweeted someone's post ranting against the government that included publicly leaked classified information? This defense is radically different from the WikiLeaks case, in which Mr. Schulte provably did not gather or transmit any classified information to WikiLeaks.

Lastly, while the MCC counts and WikiLeaks counts both involve the alleged unauthorized transmission of classified information, they are not sufficiently similar in character such that joinder is appropriate. The WikiLeaks counts charge Mr. Schulte with stealing classified information from CIA backup systems and causing that information to be provided to WikiLeaks. The MCC counts charge Mr. Schulte with communicating public information while incarcerated at MCC. As discussed above, the MCC counts are fundamentally different from the WikiLeaks counts in terms of the context in which the disclosures allegedly took place, the subject matter of the information allegedly disclosed, and the parties to whom that information was allegedly disclosed. These differences are substantial, demonstrating that the MCC counts

and WikiLeaks counts are not sufficiently similar to be joined in the same indictment. See, e.g., *United States v. Tubol*, 191 F.3d 88, 95-96 (2d Cir. 1999) (holding joinder improper, even though both charges were robberies that involved the use of a gun, because the defendant "used distinctly different methods in the two robberies" and "targeted distinctly different victims").

B. Trial should be severed so Mr. Schulte can pursue a speedy trial of the MCC Counts that are used to justify SAMs and indefinite torture

The government imposed Special Administrative Measures (SAMs) upon Mr. Schulte due to the MCC allegations, declaring him guilty and authorizing his indefinite solitary confinement and torture in a concentration camp, and therefore Mr. Schulte has a strong interest in proceeding to a speedy trial on the MCC counts. However, he cannot do so while they are improperly joined to the WikiLeaks counts—which, contrary to the MCC counts, are extraordinarily complex and involve a significant number of moving parts; Mr. Schulte is simply not yet ready for the WikiLeaks trial, but could easily defeat the government at a trial of the MCC counts 12 months ago. Accordingly, it is unconstitutional to declare Mr. Schulte guilty and to torture him without affording him the opportunity to proceed immediately to trial, prove his innocence, and ultimately remove the inhumane, barbaric SAMs.

C. Alternatively, the MCC counts should be bifurcated from the WikiLeaks counts to prevent substantial prejudice to Mr. Schulte.

Even if the court finds that joinder is proper under Rule 8(a), it should still "order separate trials or grant a severance under Rule 14 if it appears that the defendant is prejudiced by the joinder." *Werner*, 620 F.2d at 928; Fed. R. Crim. P. 14(a) ("If the joinder of offenses or defendants in an indictment... appears to prejudice a defendant or the government, the court may order separate trials of counts, sever the defendants' trials, or provide any other relief that justice

requires,"). Rule 14 is especially concerned with the danger that, when distinct offenses are tried together,

the jury may use the evidence cumulatively; that is, that, although so much as would be admissible upon any one of the charges might not have persuaded them of the accused's guilt, the sum of it will convince them as to all. This possibility violates the doctrine that only direct evidence of the transaction charged will ordinarily be accepted, and that the accused is not to be convicted because of his criminal disposition.

United States v. Lotzsch, 102 F.2d 35, 36 (2d Cir. 1939); *Werner*, 620 F.2d at 929 (acknowledging risk that multiple charges in a single trial may cause juror confusion and lead the jury to infer a criminal disposition and cumulate the evidence against the accused). Thus, when distinct offenses in an indictment "are purportedly of the same or similar character," severance is required "unless evidence of the joined offenses would be mutually admissible in separate trials" or if "the evidence is sufficiently simple and distinct to mitigate the dangers otherwise created by such a joinder." *United States v. Halper*, 590 F.2d 422, 431 (2d Cir. 1978) (citations and internal quotations omitted) (reversing joinder of Medicaid fraud and tax evasion counts).

Here, joinder of the WikiLeaks counts with the MCC counts in a single trial would severely prejudice Mr. Schulte in at least three ways. First, presenting the MCC counts necessarily would lead the jury to learn that Mr. Schulte was incarcerated pending trial on the WikiLeaks counts, highly prejudicial information that would undermine Mr. Schulte's constitutional right to a fair trial and the presumption of innocence. Second, the vast differences in the WikiLeaks and MCC counts will lead to jury confusion, as Mr. Schulte will argue the First Amendment in the MCC counts which may improperly lead the jury to believe that Mr. Schulte committed the WikiLeaks crime based on similar justification which will raise the risk that the jury will view the evidence of these charges cumulatively and convict on all counts without distinguishing between the two sets of offenses. Lastly, joinder of these offenses also prejudices

Mr. Schulte by forcing him to choose between not testifying at all, or testifying as to both the WikiLeaks counts and the MCC counts.

1. Juror knowledge of Mr. Schulte's pre-trial detention violates Due Process

The "presumption of innocence... is a basic component of a fair trial under our system of criminal justice." *Estelle v. Williams*, 425 U.S. 501, 503 (1976). In our criminal justice system, "courts must carefully guard against dilution of the principle that guilt is to be established by probative evidence and beyond a reasonable doubt." *Id.* Mr. Schulte's constitutional right to a fair trial and the presumption of innocence would be violated by presenting the MCC counts in the same trial as the WikiLeaks counts because the jury would necessarily learn that the presumption of innocence no longer exists in this country and that Mr. Schulte was presumed guilty and immediately incarcerated, and then tortured at a concentration camp, while awaiting trial on the WikiLeaks counts.

Courts have repeatedly recognized the prejudicial effect of allowing the jury to learn that the defendant is in prison. Thus, due process and the presumption of innocence forbid the government from "compelling an accused to stand trial before a jury while dressed in identifiable prison clothes." *Estelle*, 425 U.S. at 504, 512. Due process similarly "prohibit[s] the use of physical restraints visible to the jury" absent a specific state interest. *Deck v. Missouri*, 544 U.S. 622, 629 (2005); see also *United States v. Haynes*, 729 F.3d 178, 189 (2d Cir. 2013) (finding "clear error and a violation of the defendant's constitutional right to due process of law to have required the defendant [who had no prior criminal history] to stand trial in shackles without a specific finding of necessity on the record"). Consistent reference to the accused's pretrial incarceration before a jury similarly raises serious prejudice concerns that cannot be squared

with due process. *See United States v. Daoudrade*, 600 F.3d 115, 118 (2d Cir. 2010) (noting that a "constant reminder" or "extended comment" on the accused's pre-trial detention would be impermissible). Like the prison clothing that was deemed to impair the presumption of innocence fundamental to our criminal justice system, allowing the government to present evidence of Mr. Schulte's alleged misconduct at MCC during trial of the WikiLeaks counts would serve as a constant reminder of Mr. Schulte's pretrial incarceration and thus violate his right to a fair trial. This substantial prejudice alone weighs in favor of bifurcating trial on the WikiLeaks counts from the MCC counts.

2. Vast differences between the WikiLeaks counts and MCC counts would lead to juror confusion and unfair prejudice

Joinder of the WikiLeaks counts and MCC counts in a single trial raises the precise risks of unfair prejudice, confusion of the issues, and cumulative use of evidence by the jury that Rule 14 is intended to address. *See United States v. Ezeobi*, *supra*, 2011 WL 3625662, at *2 ("The danger that Rule 14 authorizes a district judge to cure is not merely that the jury will think worse of a defendant charged with two crimes rather than one, but that the jury will use the evidence cumulatively.").

Although the WikiLeaks counts and MCC counts are substantially different in purpose, time, place, and the parties involved, both sets of offenses allege the unauthorized disclosure of classified information to third parties. In fact, Mr. Schulte is charged with the same offense—illegal transmission of national defense information under 18 U.S.C. § 793(e)—for both WikiLeaks-related conduct (counts one and two) and MCC-related conduct (counts four and five). (Dkt. 405 at 1-4.) These legalistic and facial similarities between the charges raise a serious risk that the jury will view the evidence cumulatively and convict on the basis of Mr. Schulte's

primary defense in the MCC counts, that the First Amendment guarantees the right to repost public classified information already leaked on the Internet—thus improperly inferring that Mr. Schulte likely disclosed the classified information in the WikiLeaks counts as well. *See, e.g., United States v. Alvarado*, No. 92 CR 728 (LMM), 1994 WL 669968, at *3 (S.D.N.Y. Nov. 30, 1994) (“The danger of prejudicial joinder... is greater with respect to charges that are similar in character than with other types of counts properly joined under Rule 8(a).”) (Internal quotations omitted). As the Second Circuit has explained:

the only time likely saved by joinder of ‘same or similar character’ offenses is the time spent selecting a jury, and perhaps the time spent examining character witnesses. On the whole, however, the ‘trials’ on the joined charges are distinct... At the same time, the risk to the defendant in such circumstances is considerable.

Halper, 590 F.2d at 430.⁴

Moreover, in light of the complexity of the WikiLeaks charges and the large number of WikiLeaks-related counts, there is an increased risk that the jury will view the evidence cumulatively and be unable to consider the MCC counts and the WikiLeaks counts separately. For example, in *United States v. Harris*, the Court severed one fraud count relating to the defendant’s personal loan application from the remaining 22 counts on a corporate loan fraud scheme, where the “conduct is of ‘similar character’ only in the sense that each involved fraud and had the objective of persuading a bank to lend its money,” while “the risk to the defendant of unfair prejudice, through confusion of the issues or cumulative use of evidence by the jury, is heightened.” 805 F. Supp. 166, 182 (S.D.N.Y. 1992). Likewise, here, the WikiLeaks charges and the MCC charges are “similar” only in the broad sense that Mr. Schulte is accused of violating the same statute. The underlying defense, purposes, and methods for sharing that information are

⁴ Notably, time spent selecting a jury would not be “saved” by joinder here, as bifurcation of the WikiLeaks counts and MCC counts relies upon the same jury.

drastically different, and combining these two sets of charges in a single trial would likely generate juror confusion and overwhelmingly unfair prejudice, such that bifurcation is required under Rule 14.

In addition, joinder cannot be justified on the basis that evidence of the MCC counts would be admissible at trial of the WikiLeaks counts, because such evidence is inadmissible under Federal Rules of Evidence 404(b) and 403.

Federal Rule of Evidence 404(b) prohibits evidence of other crimes or bad acts as character or propensity evidence. "Other-crime evidence may be admitted if the evidence of other crimes is so distinctive that it can be seen as a 'signature' identifying a unique defendant," *United States v. Sampson*, 385 F.3d 183, 192 n.7 (2d Cir. 2004), or if relevant to another issue, such as "motive, opportunity, intent, preparation, plan, knowledge, identity, absence of mistake, or lack of accident," Fed. R. Evid. 404(b)(2). But where the defendant relies on a defense of mistaken identity—that he did not commit the crime at all—"evidence of other acts is not admissible for the purpose of proving intent." *United States v. Ortiz*, 857 F.2d 900, 904 (2d Cir. 1988).

Here, Mr. Schulte intends to assert the defense of mistaken identity with regards to the WikiLeaks charges, and there is nothing to suggest that the alleged misconduct at the MCC could be relevant to show *modus operandi*, motive, opportunity, preparation or for any other legitimate purpose. Thus, in these circumstances, evidence of any alleged misconduct at the MCC would serve no legitimate purpose at trial of the WikiLeaks counts and should be barred under Rule 404(b). See *Sampson*, 385 F.3d at 192 (holding that joinder substantially prejudiced the defendant in part because it allowed what otherwise would have been impermissible 404(b)

propensity evidence); *United States v. Krug*, 198 F. Supp. 3d 235, 251 (W.D.N.Y. 2016) ("A defendant may be substantially prejudiced... if evidence that the jury should not consider as to certain counts were nonetheless admitted in a joint trial," because "the jury might improperly use that evidence to infer a defendant's guilt as to counts on which the evidence is inadmissible").

Furthermore, even if evidence of Mr. Schulte's conduct at MCC were admissible under Rule 404(b), that evidence should be excluded under Rule 403, as its probative value would be substantially outweighed by the risk of unfair prejudice and juror confusion for the reasons stated above. *See Harris*, 805 F. Supp. at 184 (severing single fraud count from other fraud counts because even if evidence of single fraud count were admissible under 404(b), "the Rule 403 balance tips against the government in seeking to offer" that evidence at trial of the remaining fraud counts).

3. Mr. Schulte has strong reasons to testify in his defense on the WikiLeaks counts and not for the MCC counts

Prejudice arising from "when an accused wishes to testify on one but not the other of two joined offenses which are clearly distinct in time, place and evidence" will also justify severance or bifurcation under Rule 14. *Sampson*, 385 F.3d at 191 (quoting *Cross v. United States*, 335 F.2d 987, 989 (D.C. Cir. 1964)). As discussed above, the WikiLeaks counts and the MCC counts are clearly distinct in time, place, and evidence. Additionally, joinder would substantially prejudice Mr. Schulte as he has strong reasons to testify regarding the WikiLeaks counts, and not to testify on the MCC counts. At a trial on the WikiLeaks counts, Mr. Schulte would provide critical testimony in support of his defense of mistaken identity. Specifically, Mr. Schulte would testify about the facts and circumstances surrounding his employment at the CIA, including the nature of his job, the various projects he worked on, and the reasons for his conduct

with respect to specific CIA technical projects and systems. Mr. Schulte would also testify as to why the government incorrectly identified him as one of the few possible individuals who could have extracted classified information from CIA backup systems during the time period in question.

With regards to the MCC counts, the government would likely introduce Mr. Schulte's attorney-client privileged writings, taken out-of-context, and twisted into some malicious plot even though none existed; the government would similarly invoke other disingenuous twists of evidence to win at all costs—not to seek justice—such as contraband cellphones and other documents that literally have no bearing on the alleged crime itself. A defendant has a right to testify or not to testify at trial, but if he chooses to testify, he cannot selectively invoke the right to remain silent on cross-examination. *Jenkins v. Anderson*, 447 U.S. 231, 237 n.3, 238 (1980). This very dilemma substantially prejudices Mr. Schulte's constitutional right to remain silent, and separately justifies bifurcation of the WikiLeaks counts from the MCC counts.

IV. MOTION TO PRECLUDE GOVERNMENT FROM INTRODUCING TESTIMONY OR EVIDENCE DERIVED FROM FORENSIC CRIME SCENE DENIED TO DEFENSE

During the February 2020 trial, the government postulated that Mr. Schulte used his CIA computer (Workstation) to access the ESXi Server and ultimately steal digital backups from the FS01 Server. The government provided forensic images of these three servers (and much more) to its forensic experts for analysis. Mr. Schulte previously moved for access to these materials based on Fed. R. Crim. P. 16, the Fifth Amendment, the Sixth Amendment, and the *Roviano v. United States*, 353 U.S. 53 (1957), standard approved in *United States v. Aref*, 533 F.3d 72 (2d Cir. 2008). The district court denied that motion on July 22, 2019, Dkt. 124, and again on September 23, 2021, Dkt. 514, allowing the government to conceal the forensic crime scene from

the defense while relying upon it exclusively at trial. Without access to the forensic crime scene, the defense cannot rebut the government's witnesses, verify their test results, properly cross-examine them, conduct independent analysis, or subject the government's case to adversarial testing. Indeed, at the first trial, the defense wrote to the district court on February 26, 2020, Dkt. 335:

We write to advise the Court, as we have already advised the government, that the defense is unable to call its computer expert, Dr. Steven M. Bellovin, as a trial witness. As we have previously explained, Dr. Bellovin, despite repeated requests, was never permitted access to the full "mirror images" of the CIA's ESX1 and FSO1 Servers—images to which the government's expert has long been granted full and unrestricted access.

A. The Due Process Clause of the Fifth Amendment compels the government to provide equal access to private experts retained by the defense just as it does for its own experts

The Supreme Court noted in *Wardius v. Oregon*, 412 U.S. 470 (1973), that "[a]lthough the Due Process Clause has little to say regarding the amount of discovery which the parties must be afforded, ...it does speak to the *balance of forces* between the accused and his accuser." (emphasis added). Accordingly, "*Wardius* holds that rules about pretrial discovery in criminal prosecutions must apply to prosecutors as well as to defendants. Access provided to private experts retained by the prosecution must be provided to private experts retained by the defense." *United States v. Shrake*, 515 F.3d 743 (7th Cir. 2008) (emphasis added); "Fundamental fairness is violated when a criminal defendant on trial for his liberty is denied the opportunity to have an expert of his choosing, bound by appropriate safeguards imposed by the Court, examine a piece of critical evidence whose nature is subject to varying expert opinion." *Barnard v. Henderson*, 514 F.2d 744, 746 (5th Cir. 1975). The government's forensic expert, Patrick Leedom, was granted unfettered access to the alleged forensic crime scene, and in fact, all of DevLAN, to conduct his forensic examinations and investigation.

The government's forensic expert, Patrick Leedom, testified the following at trial (Tr. 1148) (bold emphasis added):

Q. And when you worked in their lab, did they give you full access to what is a full image of the FSO1 server?

A. Yes.

Q. And they gave you, did they not, access to the full image of the Atlassian server, correct?

A. That's correct.

Q. They gave you full access, did they not, to Mr. Schulte's workstation, correct?

A. Correct.

Tr. 1159-60:

Q. Let me make it easy for you. You tell me what you were given.

A. Sure. We were given images of all of the DevLAN machines -- computers, servers -- that were available at the time that we showed up to analyze.

Q. All of them, correct?

A. Yes.

Q. Now, you testified that you were also given access to the Atlassian server, right?

A. Uh, yes.

Q. And is it fair to say that the CIA gave you access all throughout the three years you worked with them on this case? Correct?

A. Yes.

Tr. 1186-87:

Q. Okay. When you examined -- did you by any chance actually physically examine any thumb drives that Mr. Schulte used?

A. I had images of those thumb drives. I've seen pictures for them, but I had forensic images of them.

Q. You had a full forensic image, correct?

A. That's correct.

Q. How many thumb drives did you have a full forensic image of?

A. A lot.

Q. A lot. How many is a lot?

A. Over the network, there were -- dozens.

Q. Right, and you had physical -- I mean, you had access to every one of those mirror images, correct?

A. Yes.

Q. In fact, you had access to the mirror images of almost every network and every computer that you needed from the CIA, correct?

A. Yes.

Q. And that very much informed your expert opinion here, correct?

A. Correct.

Since the government refuses to turn over the forensic images of the alleged crime scene—the government's very case-in-chief—including the three computers crucial to not only the espionage charges but the computer fraud and abuse charges, the government cannot simultaneously rely upon those forensic examinations while denying them to the defense; they must be precluded. "The ends of criminal justice would be defeated if judgments were to be founded on a partial or speculative presentation of the facts. The very integrity of the judicial system and public confidence in the system depend on full disclosure of all the facts, within the framework of the rules of evidence. To ensure that justice is done, it is imperative to the function of the courts that compulsory process be available for the production of evidence needed either by the prosecution or by the defense." *United States v. Nixon*, 418 U.S. 683, 709 (1974).

B. The Confrontation Clause of the Sixth Amendment

"A narrow view of Rule 16(a)(1)[(B)] is inappropriate; failure to provide reasonably available material that might be helpful to the defense and which does not pose any risks to witnesses or to ongoing investigation[s] is contrary to requirements of due process and to the purposes of the Confrontation Clause. If an expert is testifying based in part on undisclosed sources of information, cross-examination vouchsafed by that Clause would be unduly restricted." *United States v. Zanzardino*, 833 F. Supp. 429, 432 (S.D.N.Y. 1993).

Since the government's forensic experts had unfettered access to the alleged forensic crime scene, but the defense's expert did not, the defense could not effectively cross-examine the government's witnesses. The government's witnesses made bold conclusions, but their conclusions could not be verified. The defense had no ability to perform the same tests the government performed, and therefore, could not arrive at the same conclusions. The undisclosed sources of information that the government relied upon ultimately restricted the defense's cross-examination to insignificance. This inability to cross-examine resulted in a violation of the Confrontation Clause for it matters not if the Court appointed Mr. Schulte every single forensic expert in the world—if none can access the forensic crime scene to conduct a forensic examination then it's no different than refusing to appoint Mr. Schulte any expert at all. "[A] criminal trial is fundamentally unfair if the State proceeds against an indigent defendant without making certain that he has access to the raw materials integral to the building of an effective defense." *Ake v. Oklahoma*, 470 U.S. 68, 77 (1985).

Indeed, the second circuit itself has recognized the importance of full forensic images and examinations. In *United States v. Gallas*, 824 F.3d 199, 212 (2d Cir. 2016), the government argued the necessity of obtaining complete forensic images since digital data is interspersed

throughout the medium, and therefore requires analysis of the *whole* to examine any *particular* file or data. “Even the most conventional ‘files’—word documents and spreadsheets... are not maintained, like files in a file cabinet, in discrete physical locations separate and distinct from other files. They are in fact ‘fragmented’ on a storage device, potentially across physical locations.” *Gantus*, 824 P.3d at 213. “Because of the manner in which data is written to the hard drive, rarely will a file be stored intact in one place on a hard drive; so-called ‘files’ are stored in multiple forms.” *Id.* (citation omitted). “And as a corollary to this fragmentation, the computer stores unseen information about any given ‘file’—not only metadata about when the file was created or who created it, but also prior versions or edits that may still exist ‘in the document or associated temporary files on [the] disk—further interspersing the data corresponding to that ‘file’ across the physical storage medium.” *Id.* (quoting Eoghan Casey, *Digital Evidence and Computer Crime* 507 (3d ed. 2011)).

“Files,” in short, are not as discrete as they may appear to a user. Their interspersion throughout a digital storage medium, moreover, make it impossible to conduct a forensic examination without a full and complete forensic image. There is no way to know what data is relevant and critical until a full examination is performed. No professional forensic examiner ever conducts an examination without a full and complete forensic image—it would be reckless and unprofessional to attempt a forensic examination with a partial image when it is possible to utilize the entire image.

See Daniel B. Garric & Francois M. Allegra, Fed. Judicial Ctr., *Understanding Software, the Internet, Mobile Computing, and the Cloud: A Guide for Judges* 39, 40 (2015) (“Forensic software gives a forensic examiner access to electronically stored information (ESI) that is otherwise unavailable to a typical computer user... A host of information can lie in the

interstices between the allocated spaces.”), “Forensic investigators may, *inter alia*, search for and discover evidence that a file was deleted as well as evidence sufficient to reconstruct a deleted file—evidence that can exist in so-called ‘unallocated’ space on a hard drive.” *Gantlar*, 824 F.3d at 213-214. “They may seek responsive metadata about a user’s activities, or the manner in which information has been stored, to show such things as knowledge or intent, or to create timelines as to when information was created or accessed.” *Id.* at 214. See *Pharmacy Records v. Nassar*, 379 Fed. Appx. 522, 525 (6th Cir. 2010) (describing testimony of a digital forensics expert in a copyright case that the number and physical location of a file on an Apple Macintosh—which saves files sequentially on its storage medium—demonstrated that the file had been back-dated).

The government cannot have its cake and eat it too. If the government refuses to provide the defense with access to the forensic crime scene—the three computers that the government alleges Mr. Schulte used to commit the crimes—then the court must preclude the government from relying upon any and all testimony or evidence derived from these computers; the Due Process Clause simply prevents the government from relying on evidence and information that it refuses to provide to the defense for reciprocal discovery and cross-examination. Accordingly, to prevent a manifest injustice at trial (and an automatic reversal of any conviction upon review by the court of appeals), this Court must preclude the government from introducing any and all evidence, testimony, or exhibits derived from the forensic crime scene that it refused to produce to the defense.

V. MOTION TO COMPEL CLASSIFIED DISCOVERY

Judge Crotty reviewed the government’s and Mr. Schulte’s Classified Information Procedures Act, 18 U.S.C. APP. 3 (“CIPA”) Section 4 motion for access to the digital forensic

crime scene, and denied Mr. Schulte's request on July 22, 2019, Dkt. 124, and again on September 23, 2021, Dkt. 514, claiming that allowing Mr. Schulte access to the forensic crime scene is somehow too broad an access request, although it merely requested access to the three computers the government allege Mr. Schulte used to commit the crimes. Judge Crotty, however, allowed Mr. Schulte to make "more tailored requests." Dkt 514 at 3. The instant motion is a "more tailored request" for access to the CIA's Stash and Confluence backups that were allegedly stolen and transmitted to WikiLeaks, all emails and sometime messages sent and received by Mr. Schulte, and Mr. Schulte's complete CIA polygraph results.

A. Applicable Law

CIPA "establishes rules for the management of criminal cases involving classified information." *In re Terrorist Bombings of U.S. Embassies in E. Africa*, 552 F.3d 93, 115 (2d Cir. 2008). CIPA "is designed 'to protect[] and restrict[] the discovery of classified information in a way that does not impair the defendant's right to a fair trial.'" *United States v. Abu-Jihaad*, 630 F.3d 102, 140 (2d Cir. 2010) (internal citation omitted) (emphasis added). Indeed, the Supreme Court "make[s] clear that the privilege can be overcome when the evidence at issue is material to the defense." *United States v. Aref*, 533 F.3d at 79; See also *United States v. Fernandez*, 913 F.2d 148 (4th Cir. 1990) ("A finding that particular classified information is necessary to the defense is enough to defeat the contrary interest in protecting national security."). All the circuits concur and adopt "the *Roviano* standard for determining when the Government's privilege must give way in a CIPA case." *Aref* at 79 (collecting sources).

"Were it otherwise, CIPA would be in tension with the defendant's fundamental constitutional right to present a complete defense." *United States v. Fernandez*, 913 F.2d at 154; "Few rights are more fundamental than that of an accused to present witnesses in his own

defense." *Chambers v. Mississippi*, 410 U.S. 284, 302 (1973). "Any rule that impedes the discovery of truth in a court of law impedes as well the doing of justice." *Hawkins v. United States*, 358 U.S. 74, 81 (1958) (concurring opinion). The Constitution guarantees criminal defendants a meaningful opportunity to present a complete defense, and "the right to present a defense... is a fundamental element of due process of law", *Washington v. Texas*, 388 U.S. 14, 19 (1967).

"Applying [the *Roviaro*] standard, the district court must first decide whether the classified information the Government possesses is discoverable. If it is, the district court must then determine whether the state-secrets privilege applies..." *Arafat* 80 (citing state-secrets-privilege requirements as stated in *Reynolds v. United States*, 345 U.S. 1, 8, 10 (1953)).

"If the evidence is discoverable but the information is privileged, the court must next decide whether the information is helpful or material to the defense, i.e., useful 'to counter the government's case or to bolster a defense.'" *Id.* (quoting *United States v. Stevens*, 985 F.2d at 1180). "To be helpful or material to the defense, evidence need not rise to the level that would trigger the Government's obligation under *Brady v. Maryland*, 373 U.S. 83 (1963), to disclose exculpatory information." *Id.* "[I]nformation can be helpful without being 'favorable' in the *Brady* sense." *United States v. Mejia*, 448 F.3d 436, 457 (D.C. Cir. 2006).

B. Access to stolen CIA Backups

The allegedly stolen backups are proper Fed. R. Crim. P. 16 materials because they are "(i) material to preparing a defense" and "(ii) the government intends to use the item in its case-in-chief at trial." The allegedly stolen backups must be provided to the defense so the defense's forensic expert can evaluate the backups and testify at trial that they do not contain the information that was ultimately given to WikiLeaks; the defense is under no obligation to accept

the government's assertions that the data WikiLeaks published derived from the specific backup file the government claims Mr. Schulte stole. Since WikiLeaks published information that the government alleged derived from both Confluence and Stash, Mr. Schulte must be allowed access to those backups; however, Mr. Schulte is entitled not only access to the two specific backups the government alleges Mr. Schulte stole, but also access to all the Stash and Confluence backup files in the CIA's possession to conduct a timing analysis so Mr. Schulte's expert can identify and testify at trial which backup (if any) the WikiLeaks data actually originated, which would ultimately exclude Mr. Schulte as a possible suspect. Indeed, these backups are necessary to rebut the government's expert's analysis and testimony, who relied upon access to all the CIA backups to determine which he believed was the source of the WikiLeaks leak.

The government's forensic expert, Michael Berger, testified to this "Timing analysis." (Tr. 1351-52):

Q. Were you asked to conduct any analysis of the BDG information disclosed by WikiLeaks?

A. Yes, I was.

Q. Have you formed any opinions with respect to that information?

A. Yes, I have.

Q. What opinions have you formed?

A. I was asked to perform analysis and conduct a timing analysis and look at the data that was on WikiLeaks. My opinion of that analysis is that the data that was released on WikiLeaks came from a date range between March 2 and March 3, 2016.

Q. Was there a backup in existence on the Confluence -- was there a Confluence backup file in existence on DevLAN within that time range?

A. Yes.

Q. Which one was that?

A. It was the March 3 backup.

Q. So, if we go to the next slide and move on to the next one after that, I'd like to start with how you arrived at that opinion. Could you describe your methodology, please?

A. Sure. So, I was asked to look at the data that was on WikiLeaks and determine when it came from in the Confluence system. In order to do that, we looked at the concept of version control, which both Stash and Confluence employ. Version control is a basic ability where you can make up dates to documents or source code. And when you save them, they don't completely overwrite your previous versions. The system keeps track of the history of versions so it goes from version 1, version 2.

[...]

Q. I'm sorry to interrupt.

A. That's okay. Because we knew that the version control existed on those systems, we could look at activity that happened on those systems and we could look at data that was posted on WikiLeaks. We then looked for examples of data points of data that was saved in the system that was present on WikiLeaks. And data that was saved in the system that was not present on WikiLeaks.

At trial, the government's forensic expert, Michael Berger, utilized his unfettered access to all the Stash and Confluence backups to conduct a timing analysis. Berger's analysis could not be cross-examined, verified, or challenged because the defense did not have access to the backups, and therefore could not reproduce Berger's timing analysis. Since the government's case depends upon Berger identifying one specific backup file as the originating data, if the defense were given access to the backups and Mr. Schulte's forensic expert could rebut the government's expert and identify any *other* backup file as the originating data, or even *none*, then Mr. Schulte must be acquitted. Accordingly, access to the CIA's Stash and Confluence

backups is both material to preparing a defense and relied upon by the government in its case-in-chief. It must be provided to the defense.

The necessity of the Stash and Confluence backups easily defeats the classified nature of the discovery. There can be no question that the backups are fundamental to the government's case and critical to the defense—they are literally the crux of the government's case. The defense must be permitted unfettered access to these backups to properly prepare a defense—just as the government relied upon them to further its prosecution.

Finally, the government's argument is diminished since the defense does not seek declassification of the data, but only production to the defense's fully-cleared forensic expert and the defendant—who the government already acknowledged had unfettered access to the materials when he worked at the CIA. Moreover, the files were already leaked and transmitted to Wikileaks. So, further exposure of the same data to the defendant poses no new threat to national security.

C. Access to CIA emails and Sametime messages sent and received by Mr. Schulte, including all metadata

The government's theory is that Mr. Schulte was a disgruntled employee. In order to rebut this argument, the government must produce all emails and Sametime messages both sent and received by Mr. Schulte. These messages and associated metadata are also critical in establishing timelines that the defense intends to introduce at trial to rebut the government's case; the metadata includes times Mr. Schulte logged into, accessed, read, and drafted emails. The content must be provided to the defense in its native format to preserve metadata and other important data points.

D. Access to CIA Polygraph and results

The government must produce all "reports of examinations and tests." Fed. R. Crim. P. 16(F). This includes Mr. Schulte's polygraph and background examination. While the government previously provided the polygraph transcript, it has yet to provide the actual polygraph test results (i.e. the logged heart rate, oxygen, and other readings), along with the polygrapher's written notes and ultimate determination. Note that these records are proper Rule 16 materials that must be provided to the defense whether or not the government believes them to be ultimately inadmissible at trial.

Moreover, Mr. Schulte intends to introduce the CIA polygraph at trial to demonstrate that the CIA exonerated him of any wrongdoing through its own internal testing; that the CIA trusts its polygraph and background investigation. While polygraphs typically are not admissible in court, the context is vastly different here. Additionally, the CIA polygraph is substantially different from the typical polygraph, and Mr. Schulte is entitled to the CIA's vast trove of polygraph and scientific data so he can demonstrate to the Court the effectiveness and superiority of the CIA's polygraph. It is a technological improvement that requires additional briefing before the court; Mr. Schulte will ultimately move for its introduction at trial.

**VI. MOTION TO SUPPRESS NON-RESPONSIVE AND ATTORNEY-CLIENT
PRIVILEGED DOCUMENTS SEIZED FROM MCC**

On October 3, 2018, the FBI executed a search warrant at the MCC to seize nine documents identified only by their titles; however, instead of adhering to the particularity described in the warrant, the FBI helped themselves to all of Mr. Schulte's notebooks, including those marked "Attorney-Client Privilege," and conducted a general search and exploratory rummaging through all of Mr. Schulte's documents. Instead of filtering the documents based on privilege and responsiveness to the search warrant, the government merely seized every

document, searched every sentence, and provided all to the CIA to conduct a comprehensive classification review. The FBI went into Mr. Schulte's home with a warrant to seize 9 specific documents, but indiscriminately seized everything instead. "And enshrined in the Fourth Amendment is the fundamental principle that the Government cannot come into one's home looking for some papers and, without suspicion of broader criminal wrongdoing, indiscriminately take all papers instead." *Boyd v. United States*, 116 U.S. 616, 626-27 (1886). This Court should now suppress the non-responsive and attorney-client privileged documents.

A. Attorney-Client Privilege

"The attorney-client privilege protects communications (1) between a client and his or her attorney (2) that are intended to be, and in fact were, kept confidential (3) for the purpose of obtaining or providing legal advice." *United States v. Finazzo*, 682 Fed. Appx. 6, 15 (2d Cir. 2017) (quoting *United States v. Mejia*, 655 F.3d 126, 132 (2d Cir. 2011)). "The attorney-client privilege protects confidential communications between client and counsel made for the purpose of obtaining or providing legal assistance." *ACLU v. NSA*, 925 F.3d 576, 589 (2d Cir. 2019) (quoting *Pritchard v. County of Erie (In re County of Erie)*, 473 F.3d 413, 418 (2d Cir. 2007)). The privilege functions to "encourage attorneys and their clients to communicate fully and frankly and thereby to promote broader public interests in the observance of law and administration of justice." *Id.*; see also *Upjohn Co. v. United States*, 449 U.S. 383, 389 (1981) (explaining that one purpose of the privilege is "to encourage clients to make full disclosure to their attorneys" (internal quotation marks omitted)). It is "well settled that individuals retain their attorney-client privilege when incarcerated or detained." *United States v. Mejia*, *supra*. See also *United States v. Defonte*, 441 F.3d 92, 94 (2d Cir. 2006) (*per curiam*); *Gomez v. Vernon*, 255

F.3d 1118, 1133 (9th Cir. 2001) (finding that prisoners retain right to keep privileged documents confidential where not inconsistent with legitimate penological interests).

B. Seizure and search of Non-Responsive documents

The Fourth Amendment explicitly commands that warrants must be based on probable cause and must "particularly describ[e] the place to be searched, and the persons or things to be seized," U.S. Const. amend. IV. "It is familiar history that indiscriminate searches and seizures conducted under the authority of 'general warrants' were the immediate evils that motivated the framing and adoption of the Fourth Amendment," *Payton v. New York*, 445 U.S. at 583. Those general warrants "specified only an offense," leaving "to the discretion of the executing officials the decision as to which persons should be arrested and which places should be searched." *Stegald v. United States*, 451 U.S. at 220. The principal defect in such a warrant was that it permitted a "general, exploratory rummaging in a person's belongings," *Andresen v. Maryland*, 427 U.S. 463, 480 (1976) (internal quotation marks omitted), a problem that the Fourth Amendment attempted to resolve by requiring the warrant to "set out with particularity" the "scope of the authorized search," *Kentucky v. King*, 563 U.S. at 459. This requirement "'makes general searches... impossible and prevents the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant.'" *Stanford v. Texas*, 379 U.S. at 485 (quoting *Marron v. United States*, 275 U.S. 192, 196 (1927)).

The unauthorized seizure of voluminous material not specified in the warrant and the retention of the seized documents clearly violates the Fourth Amendment. *United States v. Tamura*, 694 F.2d 591, 595, 597 (9th Cir. 1982); see also, *supra*, *Andresen v. Maryland*, 427 U.S. at 482 n.11 ("[W]e observe that to the extent [seized] papers were not within the scope of the

warrants or were otherwise improperly seized, the State was correct in returning them voluntarily and the trial judge was correct in suppressing others... In searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized... [R]esponsible officials [conducting such searches], including judicial officials, must take care to assure that they are conducted in a manner that minimizes unwarranted intrusions upon privacy."); cf. *United States v. Matias*, 836 F.2d 744, 747 (2d Cir. 1988) ("[W]hen items outside the scope of a valid warrant are seized, the normal remedy is suppression and return of those items..."); *United States v. Dalalok*, 441 F.2d 212, 216 (2d Cir. 1971) ("[T]he law in this area is quite clear... if something is not described in the warrant it cannot be seized.")

C. Suppression of specific documents

Contrary to the government's claims, this issue has not previously been addressed by the Court—in fact, there was a months-long discussion of attorney-client privilege, advice-of-counsel defense, and a conflict-of-interest that required a *Cureto* hearing. Much of this is changed now that Mr. Schulte is *pro se*.

The government claimed in its November 18, 2021 letter that the instant motion was already addressed by the defense's motion in *limine*, Dkt. 242. There, the defense requested wholesale suppression of all the MCC notebooks based on attorney-client privilege and requested the Court relieve them as counsel due to an actual conflict-of-interest due to the privilege and advice-of-counsel. *Id.* at 23–24. The Court ordered the government to identify the notebook entries it intended to use at trial, Dkt. 252. The government asked to preclude the advice-of-counsel defense and listed the proposed MCC documents it intended to use at trial, Dkt. 257. However, the conflict-of-interest became a major issue before trial. Dkt. 128, 150, 154,

157, 164, 166, 181 (appointment of *Curcio* counsel), 218 (re: *Curcio* hearing), 220 (ineffective assistance of counsel), 221, 232 (purported waiver of attorney-client privilege), 233 (disqualification recommendation from *Curcio* counsel), 241, 244, 245, 248, 249, 253. A *Curcio* hearing was held on December 18, 2021, in which Mr. Schulte did not waive the actual conflict-of-interest. Judge Crotty overruled *Curcio* counsel and ordered the defense to disclose attorney-client privilege to the government. Dkt. 248. The defense did not do so due to the conflict-of-interest, so Judge Crotty ordered preclusion of the advice-of-counsel defense and other defense reliance on attorney-client privilege (ultimately precluding Mr. Schulte's testimony at trial as it was ordered he could not testify about his "state-of-mind," thus the actual conflict-of-interest subjects the misdemeanor convictions to automatic reversal, consistent with clearly established second circuit law). Dkt. 259. Now that Mr. Schulte represents himself, he will raise the advice-of-counsel defense at trial, call his former attorneys as fact witnesses, and introduce evidence that several documents were protected by attorney-client privilege—including *Malware of the Mind*. So, there is no "reconsideration" requested here, but rather a complete change in defense strategy and circumstances; and even if it were interpreted as a "reconsideration," the new facts support reconsideration.

Finally, the issue of suppressing non-responsive documents illegally seized pursuant to the MCC search warrant was never addressed by the Court. The Court should thus review and ultimately suppress the following documents.

1. *Malware of the Mind*

Since Mr. Schulte wrote *Malware of the Mind* exclusively for his attorneys, and only ever shared it with them, for the sole purpose of his defense, the document is protected by Attorney-Client Privilege, and must be suppressed. Additionally, *Malware of the Mind* was not one of the

nine identified files in the search warrant, and a cursory review of the document revealed no classified information; accordingly, the government was not authorized to seize this document.

n) Malware of the Mind: A History

Mr. Schulte wrote *Malware of the Mind* in March of 2018 exclusively for his newly assigned attorneys. As is the case with all attorney-client work product and privileged information that Mr. Schulte wrote, *Malware of the Mind* was written in narrative format—the government previously seized several attorney-client privileged documents dating back to March of 2017 in which Mr. Schulte wrote information exclusively for his attorneys in a narrative format, but which was never shared, published, or ever intended to be published, thereby firmly establishing this practice.

After finishing with the document, Mr. Schulte mailed it to Hannah Sotnick, a paralegal with the Federal Defenders of New York, asking her to give it to counsel and to give him any advice about the document. She made copies and distributed it to Mr. Schulte's attorneys. She then mailed Mr. Schulte back both the original and a copy that contained hand-written commentary from either another representative of the Federal Defenders. The copy was incomplete, and Mr. Schulte sent her back the original and asked her if she could finish a complete copy. She then made a complete copy and mailed Mr. Schulte that copy while maintaining the original. That photocopy of *Malware of the Mind* remained inside the Federal Defenders envelope it was mailed in until the FBI illegally opened it and seized the document although the search warrant did not identify envelopes from the Federal Defenders nor *Malware of the Mind* to seize.

After the government falsely claimed *Malware of the Mind* was "classified," Mr. Schulte's attorneys brought the original to the SCIF in an abundance of caution, where it remains

to this day. The government's seized photocopy would perfectly match the original document that remained in Mr. Schulte's attorney's possession as it was written exclusively for them.

Half a year after *Malware of the Mind* was written, Mr. Schulte contemplated writing a tenth and final article in his *unclassified* redress of grievances criticizing the federal government and its corrupt criminal justice system. Mr. Schulte always liked the title "*Malware of the Mind*" and the associated introductory paragraph which was originally written for Omar Amanat's technical report (long before "*Malware of the Mind*"), and considered reusing this paragraph as the opening for the final article. However, as the *unclassified* articles were about the corrupt, diabolical American criminal "just us" system, the content would obviously differ completely. This is why page 125 of "*Red_Notebook_-_Gen_7.25-9 - UNCLASSIFIED*" (2019.05.29 production), Ex. B, *AND* Trial Exhibits 809, Ex. C, at 8, specifically states "~~rewrite~~ *Malware of the Mind*." Ultimately, Mr. Schulte scrapped the idea for a tenth article entirely as he felt the nine were sufficient for his purposes.

The FBI stopped nothing. In fact, Mr. Schulte's redress of grievances was published on the internet after they seized the cell phone allegedly belonging to Mr. Schulte (although it was found in another inmate's cell). Indeed, it was impossible for Mr. Schulte to have published anything on the internet as he was already in solitary confinement *before* it was published.

Regardless, the "*Malware of the Mind*" illegally seized and searched by the FBI was drafted for, and only ever transmitted to, Mr. Schulte's attorneys, for the express and sole purpose of aiding his criminal defense and preparing for trial.

See Ex. D, "Schulte Declaration."

b) Malware of the Mind Is Attorney-Client Privileged material and should be suppressed

Malware of the Mind was written as a confidential document disclosed only to Mr. Schulte's attorneys to assist in his legal defense. "Confidential disclosures by a client to an attorney made in order to obtain legal assistance are privileged." *Fisher v. United States*, 425 U.S. 391, 403 (1976). See *United States v. DeForte*, 441 F.3d at 96 (finding attorney-client privilege would apply to writings from a journal that has been taken from an inmate's cell at the MCC so long as those writings were an outline of what the inmate wished to, and ultimately did, discuss with counsel); *Clark v. Buffalo Wire Works Co.*, 190 F.R.D. 93, 96-97 (W.D.N.Y. 1999) (notes client made "in order to inform an attorney about facts from his daily life that he considered to be relevant to his potential legal remedies" were protected by attorney-client privilege); *Bernbach v. Timex Corp.*, 174 F.R.D. 9, 9-10 (D. Conn. 1997) (notebooks written by client containing "almost daily notes of events and conditions in her life which she felt were critical for her attorneys to know" satisfied the elements of attorney-client privilege).

Additionally, Malware of the Mind remained completely confidential, and was not shared with anyone outside counsel. "[I]t is vital to a claim of privilege that the communications between client and attorney were made in confidence and have been maintained in confidence." *In re Horowitz*, 482 F.2d 72, 81-82 (2d Cir. 1973). Moreover, the person invoking the privilege must have taken steps to ensure that it was not waived—"It is not asking too much to insist that if a client wishes to preserve the privilege..., he must take some affirmative action to preserve confidentiality," *Id.* at 82. Thus, "the question of whether the privilege applies... involve[s] a determination of whether the claimant asserting the privilege treated the communications in question in such a careless manner as to negate her or her intent to keep them confidential," *Mejia*, 655 F. 3d at 132-33 (alterations and internal quotation marks omitted); see also *DeForte*,

supra, at 94-95 (noting that attorney-client privilege would be waived if the claimant treated documents as issue “in such a careless manner as to negate her intent to keep them confidential”). It is abundantly clear that Mr. Schulte sought to protect Malware of the Mind by keeping it in the original envelope sent by the Federal Defenders and marked as “Attorney-Client Privilege.” There was nothing more Mr. Schulte could have done to preserve privilege.

To the degree that the specific introductory paragraph of Malware of the Mind was privileged, it is clear that this paragraph was written *before* Malware of the Mind, was not written to Mr. Schulte’s attorneys, was included in public documents, and therefore it was never privileged. However, including a public paragraph in Malware of the Mind does not nullify privilege of that document—at most, the public paragraph remains public, but that taint does not infect the Malware of the Mind document. “Public, even extrajudicial, disclosures constitute a waiver of the privilege for the communications or portions of communications disclosed.” *United States v. Jacobs*, 117 F.3d 82, 91 (2d Cir. 1997) (emphasis and internal quotation marks omitted), *abrogated on other grounds by Loughrin v. United States*, 134 S. Ct. 2384 (2014).

Finally, it’s critical to note, once again, that the Malware of the Mind document was a photocopy created by Mr. Schulte’s attorneys for him to maintain in his confidential records while his attorneys maintained his original document. That photocopy remained within the protected legal mail for over 7 months until the FBI perverted its search warrant into an illegal general warrant and seized it. See *Davis v. Goorn*, 320 F.3d 346, 351 (2d Cir. 2003) (noting that “courts have consistently afforded greater protection to legal mail than to non-legal mail.”); see also *Saffler v. Brooks*, 343 F.3d 868, 874 (6th Cir. 2003) (recognizing “heightened concern” with allowing prison officials to open and read mail that “has import for... the attorney-client privilege”).

Suppression is warranted when evidence is obtained in violation of the Sixth Amendment or the Attorney-Client privilege. See, e.g., *United States v. Longo*, 70 F. Supp. 2d 225, 264 (W.D.N.Y. 1999) ("Where a violation of the attorney-client privilege is demonstrated, the remedy for such a violation is the suppression of evidence derived from the privileged communication."). "Unquestionably, government interference in the relationship between attorney and defendant may violate the latter's right to effective assistance of counsel." *United States v. Ginsberg*, 758 F.2d 823, 833 (2d Cir. 1985) (citing *Massiah v. United States*, 377 U.S. 201 (1964)). Accordingly, the FBI's seizure of Mr. Schulte's legal mail and subsequent search of documents clearly marked as Attorney-Client privileged was unconstitutional. The Malware of the Mind document must be suppressed.

c) Malware of the Mind was not responsive to the search warrant

Finally, Malware of the Mind was not responsive to the MCC search warrant to search and seize 9 unclassified documents produced to Mr. Schulte is unclassified discovery; the FBI had no knowledge of Malware of the Mind, and did not seek to seize it. The FBI's seizure of the entire document despite no specification in the warrant—without conducting a review of responsive and non-responsive pages—and subsequent production of the entire document to the CIA to conduct a comprehensive classification review of the entire document necessitates wholesale suppression of the entire document. As the Court can see in *ex parte* Ex. B-1, B-2, and B-3, a cursory review of Malware of the Mind should not have triggered seizure.

2. Red notebook labeled "7/25 -9/1"

This entire notebook is attorney-client privileged; Mr. Schulte clearly wrote "ATTORNEY CLIENT PRIVILEGE" in boldface on the outside and inside covers (appears unmistakably in originals). See OX 809, Ex. C. See also OX 806, Ex. F.

Contrary to the government's belief, a search warrant does not grant the government the ability to conduct a general search and seizure of anything that they wish to use at trial; the document must first be categorized into responsive and non-responsive materials. The government never did this. Indeed, this notebook and all pages therein are not responsive to the MCC search warrant, which sought the seizure of 9 unclassified documents by their titles alone. This notebook contained no such titles or documents; it should not have been seized nor searched.

a) Passwords page, GX 809 p. 6; GX 806 p. 8

This page of passwords is attorney-client privileged; Mr. Schulte wrote and transmitted known passwords and accounts to his attorneys. Such information is typically privileged. Furthermore, the password page is not responsive to the MCC search warrant; it does not contain the nine titles sought in the search warrant nor does it reference them at all. Accordingly, this page and all information derived therefrom must be suppressed.

b) "\$50 Billion" GX 809 p. 2; GX 806 p. 4

The \$50 billion statement must be suppressed because it is a direct quote and recitation of the communication between Mr. Schulte and his attorney:

If govt doesn't pay me \$50 billion in restitution & prosecute the criminals who lied to the judge and presented this BS case then I will visit every country in the world and bear witness to the treachery that is the USO. I will look to breakup diplomatic relationships, close embassies, end U.S. occupation across the world & finally reverse U.S. jingoism. If this is the way the U.S. govt treats one of their own, how do you think they will treat allies?

This statement is not about "blackmailing" the government, but rather, about the corrupt "justice" system and Mr. Schulte's intentions to "bear witness to the treachery that is the USO", i.e. the government's continual lies and deception about Mr. Schulte. As the Court can see, much of this page (and the next multiple pages) were redacted for attorney-client privilege as it is

verbatim dialogue between client and attorney—this is literally what Mr. Schulte told his attorney; that the government desired to exclude this salacious statement that they may disingenuously twist it out-of-context to use at trial does not exclude it from privilege; compare the version redacted for privilege, Ex. G-1 with the full, verbatim recitation in classified *ex parte* Ex. G-2. Moreover, nothing in the statement is illegal that would negate privilege. Mr. Schulte still intends that, after acquittal, he will visit every country in the world to bear witness to the treachery that is the USG—he will describe his torture at United States concentration camps for a duration exceeding WWII, how the United States is the greatest terrorist organization that this world has ever seen, and urge every government to halt all extraditions to the United States, embargo all U.S. products, blockade all U.S. trade, halt use of the U.S. dollar, and terminate all diplomatic relationships with the United States until it ends all concentration camps and submits to an international tribunal to judge all federal prosecutors, federal judges, and Department of Justice officials for their role in the human rights atrocities committed at their hands—the Great American holocaust. Mr. Schulte has every right to discuss these intentions with his attorney, to obtain feedback, legal advice, and even to execute these intentions.

Furthermore, this page is not responsive to the MCC search warrant; it does not contain the nine titles sought in the search warrant nor does it reference them at all. Accordingly, this page and all information derived therefrom must be suppressed.

c) *"Information War" GX 809 p. 3-4, 7-8, 14-16; GX 806 p. 5-6, 9-10, 16-18*

Mr. Schulte's "information war" against the government—his self-described war against the government's lies and deception about him—fought with the truth, is an attorney-client privileged strategy. Mr. Schulte initiated this "war" with assistance from his family in posting his

unclassified articles critical of the U.S. criminal "justice" system—the most diabolical and corrupt system on Earth. Mr. Schulte's strategy and interaction with the media and the press is an attorney-client privileged strategy, protected from the government. Mr. Schulte has a First Amendment right to discuss his case and to issue a redress of grievances to the corrupt, despicable government, and to wage an information war for the truth.

Furthermore, these pages are not responsive to the MCC search warrant; they do not contain the nine titles sought in the search warrant, they do not reference classified information, nor do they ever even remotely propose releasing classified information as part of the "war." Accordingly, these pages and all information derived therefrom must be suppressed.

d) Checklist GX 809 p. 5; GX 806 p. 7

This page is not responsive to the MCC search warrant; it does not contain the nine titles sought in the search warrant nor does it reference them at all. Accordingly, this page and all information derived therefrom must be suppressed.

e) Supposed Planned Tweet, GX 809 p. 9-13; GX 806 p. 11-15

These page are not responsive to the MCC search warrant; they do not contain the nine titles sought in the search warrant nor do they reference them at all. Accordingly, these pages and all information derived therefrom must be suppressed.

3. Other Notebooks

a) GX 806 p. 1

This entire page is attorney-client privileged, in which Mr. Schulte writes reminders and information to his attorneys. See classified, *ex parte* Ex. H. The government took the middle of this page out-of-context from the other attorney-client privileged information. Here, Mr. Schulte writes to his attorneys to query Wikileaks if they possess software he developed to assist in his

own defense since the government refused to turn over any of it in discovery; since the government continues to conceal exculpatory evidence from the defense, they must try anything to obtain it. It is absolutely unconscionable that the government sought to use this clearly privileged information against Mr. Schulte.

Furthermore, this page is not responsive to the MCC search warrant; it does not contain the nine titles sought in the search warrant nor does it reference them at all. Accordingly, this page and all information derived therefrom must be suppressed.

b) GX 806 p. 2-3

See, *supra*, 2.c. Mr. Schulte's decision to publicly release an unclassified redress of grievances is an attorney-client privileged defense strategy; the government has no business prying into this strategy.

Furthermore, this page is not responsive to the MCC search warrant; it does not contain the nine titles sought in the search warrant. Accordingly, this page and all information derived therefrom must be suppressed.

VII. CONCLUSION

The court should grant Mr. Schulte's requested relief with regards to his motion (1) to suppress evidence seized from Google, Github, and Reddit; (2) for severance / bifurcation of trial; (3) to preclude the government from introducing testimony or exhibits derived from the forensic crime scene denied to the defense; (4) to compel classified discovery; (5) to suppress non-responsive and attorney-client privileged documents seized from MCC.

Dated: New York, New York

January 24, 2022

Respectfully submitted,

Joshua Adam Schulte

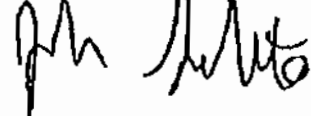


EXHIBIT A

17 MAG 6961

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK**

**In the Matter of an Application for
Search Warrants for Stored Electronic
Communications**

**SEALED
AGENT AFFIDAVIT**

____ Mag. ____

**Application for Search Warrants
for Stored Electronic Communications**

**STATE OF NEW YORK)
) ss.
COUNTY OF NEW YORK)**

JEFF D. DONALDSON, being duly sworn, deposes and states:

I. Introduction

1. I am a Special Agent of the Federal Bureau of Investigation ("FBI") assigned to the New York Field Office, and have been employed by the FBI since 2010. I am currently assigned to a squad responsible for counterespionage matters and have worked in the field of counterintelligence from 2010 to present. In the course of my duties as a Special Agent, I am responsible for investigating offenses involving espionage and related violations of law, including unauthorized retention, gathering, transmitting or losing classified documents or materials; unauthorized removal and retention of classified documents or materials; illegally acting in the United States as a foreign agent; other national security offenses; and the making of false statements. As a result of my involvement in espionage investigations and investigations involving the unauthorized disclosure or retention of classified information, as well as my training in counterintelligence operations, I am familiar with the tactics, methods, and techniques of United States persons who possess, or have possessed a United States Government security clearance and may choose to harm the United States by misusing their access to classified

USG-CONFIDENTIAL

JAS_000094

Information. I am also familiar, through my training and experience with the use of computers in criminal activity and the forensic analysis of electronically stored information.

2. **Basis for Knowledge.** This Affidavit is based upon my participation in the investigation, my examination of reports and records, and my conversations with other law enforcement agents and other individuals, as well as my training and experience. Because this Affidavit is being submitted for the limited purpose of obtaining the Requested Information, it does not include all the facts that I have learned during the course of this investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated. In addition, unless otherwise indicated, statements by others referenced in this Affidavit were not necessarily made to me, but may have been provided to me by someone else to whom I have spoken or whose report I have read (and who in turn may have had either direct or indirect knowledge of the statement). Similarly, unless otherwise indicated, information in this Affidavit resulting from surveillance does not necessarily set forth my personal observations, but may have been provided to me by other law enforcement agents who observed the events, and to whom I have spoken or whose report I have read.

II. The Target Accounts

3. I make this affidavit in support of an application for search warrants pursuant to 18 U.S.C. § 2703 directed to Google, Inc., headquartered in Mountain View, CA ("Google"); Reddit, Inc., headquartered in San Francisco, CA ("Reddit"), and Github.com, headquartered in Sacramento, CA ("GitHub"), (collectively, "Providers"), for all content and other information associated with the following "Target Accounts":

a. The Google account associated with the email address **joshshultel@gmail.com** (the "Subject Google Account"), which is maintained and controlled by Google.

b. The Reddit account associated with the account name **L1347517** (the "Subject Reddit Account"), which is maintained and controlled by Reddit.

c. The GitHub account associated with the user name **pedbaktb11** (the "Subject GitHub Account"), which is maintained and controlled by GitHub.

4. The information to be searched is described in the following paragraphs and in Attachment A to each of the proposed warrants.

Google

5. Based on my training, experience, and participation in this investigation, I know the following about Google:

a. Google offers email and other Internet-based services to the public. Among other things, Google allows subscribers to maintain email accounts under the domain name **gmail.com**. A subscriber using Google's services can access his or her email account from any computer connected to the Internet, and can link any variety of Google's other Internet-based services to his/her Gmail account.

b. Google maintains the following records and information with respect to every subscriber account:

i. *Email contents.* In general, any email (which can include attachments such as documents, images, and videos) sent to or from a subscriber's account, or stored in draft form in the account, is maintained on Google's servers unless and until the subscriber deletes the email. If the subscriber does not delete the email, it can remain on Google's computers

Indefinitely. Even if the subscriber deletes the email, it may continue to be available on Google's servers for a certain period of time.

ii. *Address book.* Google also allows subscribers to maintain the equivalent of an address book, comprising email addresses and other contact information of other email users.

iii. *Subscriber and billing information.* Google collects and maintains (typically unverified) identifying information about each subscriber, including, for example, name, username, address, telephone number, and alternate email addresses. Google also maintains records concerning the date on which the account was created, the Internet protocol ("IP") address of the user at the time of account creation, the current status of the account (e.g., active or closed), the length of service, and the types of services utilized by the subscriber. Additionally, for paying subscribers, Google maintains records of the subscriber's means and source of payment, including any credit card or bank account number.

iv. *Transactional information.* Google also typically retains certain transactional information about the use of each account on its system. This information can include records of login (i.e., session) times and durations and the methods used to connect to the account (such as logging into the account through Google's website).

v. *Customer correspondence.* Google also typically maintains records of any customer service contacts with or about the subscriber, including any inquiries or complaints concerning the subscriber's account.

vi. *Preserved records.* Google also maintains preserved copies of the foregoing categories of records with respect to an account, for at least 90 days, upon receiving a preservation request from the Government pursuant to 18 U.S.C. § 2703(f).

e. In addition, subscriber information for the Subject Google Account indicates that the subscriber of the Subject Google Account has activated additional online Google Services, and; accordingly, the Provider also maintains, among other things, the following records and information with respect to the Subject Google Account:

i. *Google Drive*. Google provides users with a certain amount of free "cloud" storage, currently 15 gigabytes, through the service called "Google Drive" (users can purchase a storage plan through Google to store additional content). Users can use their Google Drive to store email, attachments, videos, photographs, documents, and other content "in the cloud," that is online. A user can access content stored on Google Drive by logging into his or her Google account through any computer or other electronic device that is connected to the Internet. Users can also share files stored on Google Drive with others, allowing them to view, comment, and/or edit the files.

ii. *Google Docs*. Google provides users with the ability to write, edit, and collaborate on various documents with other Google users through a service called "Google Docs." Users can use Google Docs to create online documents that can be stored on or saved to the user's Google Drive. Users can also download such documents in various formats, such as a Microsoft Word document (e.g., ".docx"), an OpenDocument Format (".odt"), Rich Text Format (".rtf"), a PDF document (".pdf"), or Plain Text document (".txt").

iii. *Google Photos*. Google provides users with a certain amount of free storage for photographs, through a service called Google Photos, which allows users to manually store photographs and videos, and which automatically uploads photographs and videos taken by registered mobile devices. Google also retains the metadata—or data that provides information about the data in question, such as the time and date of creation, the author or creator, the means

of its creation, the purpose of the data, among other data—for photos and videos that are uploaded to Google, including to Google Photos. This metadata includes what is known as exchangeable image file format (or “Exif”) data, and can include GPS location information for where a photo or video was taken.

iv. *Google Calendar.* Google provides users with an online calendar, in which they can add appointments, events, and reminders, which are synchronized across registered computers and mobile devices. Users can share their calendars with other users, allowing the maintenance of joint calendars.

v. *YouTube content.* Google allows subscribers to maintain linked YouTube accounts, a global video-sharing website that allows users to upload and share videos with public on the Internet. Registered users can upload an unlimited number of videos and add comments to videos.

vi. *Google Chats and Google Hangouts content.* Google allows subscribers to engage in “chat” sessions in an instant messaging format with other Google users, the transcripts of which are generally stored in a user’s email content. Similarly, Google allows users to engage in enhanced chat sessions, called Hangouts, which permit the sharing of additional content such as videos, sounds, and images. In general, Hangouts content is stored separately from a user’s email and chat content.

vii. *Location History data.* Google maintains recent location data, collected periodically, from mobile devices that are logged into or have used applications (or “apps”) or services provided by Google. For example, Google collects information collected from GPS, Wi-Fi networks, cell site locations, and mobile networks to estimate a user’s location.

Google apps and services also allow for location reporting, which allows Google to periodically store and use a device's most recent location data in connection with a Google account.

viii. *Android Services.* Google also maintains information relating to Android, as it relates to an account. Android is a mobile operating system that is developed by Google, and is used on a variety of touchscreen mobile devices, such as smartphones and tablet computers. Google retains information related to the Android device associated with an account, including the IMEI (the International Mobile Station Equipment Identifier), MEID (the Mobile Equipment Identifier), device ID, and/or serial number of the devices. Each of those identifiers uniquely identifies the device used. One device may be associated with multiple different Google and Android accounts, and one Google or Android account may be associated with multiple devices.

ix. *Google Voice.* Google provides a telephone service that provides call forwarding and voicemail services, voice and text messaging.

x. *Google Payments.* Google allows for the storage of payment information associated with a Google Account, including credit cards and bank accounts, and contains information about all transactions made with a Google account, allowing for the payment for goods (such as those purchased through Google Shopping) and bills, among other features.

xi. *Web History.* Google maintains searches and account browsing activity, from Chrome, Google's proprietary web browser, as well as other Google applications.

Reddit

6. Based on my training, experience, and participation in this investigation, I know the following about Reddit:

a. Reddit operates several products and services, including reddit.com, redditgifts.com, and associated Reddit mobile applications. The most popular product is reddit.com, which provides an online forum where people can create communities (known as "subreddits") in which users can communicate online.

b. Each subreddit on reddit.com has its own page, subject matter, users, and moderators. Users post stories, links, and media to these communities, and other users can comment and can "upvote" or "downvote" a post.

c. The information that is collected by Reddit varies depending on what services the user utilizes. For example, if the user signs up to post on the website reddit.com, Reddit users can choose to provide their name and other contact information (including, but not limited to, their email address), although though users can also choose not to do so. If the user signs up to Reddit Gifts, the user may be asked to provide Reddit with personal information such name, address, telephone number, age, personal interests, and email address. The user may also be required to provide log-in information for an existing Reddit Account or to create one before using Reddit Gifts.

GitHub

7. Based on my training, experience, and participation in this investigation, I know the following about GitHub:

8. Based on my training, experience, and participation in this investigation, I know the following about GitHub:

a. GitHub is a web-based Git, or version control repository, and Internet-hosting service, that can be accessed at <https://github.com/>. GitHub allows Internet users to host code, manage projects, and build software alongside millions of other developers.

b. A user must create an account in order to contribute content to the site, but public repositories can be browsed and downloaded by others. When an individual registers for an account, they are able to discuss, manage, create repositories, submit contributions to others' repositories, and/or review changes to code. Users are represented in GitHub's system as personal GitHub accounts. Each user has a personal profile, and can own multiple repositories. Users can create or be invited to join organizations, or to collaborate on another user's repository. A repository is one of the most basic GitHub elements. It can contain project files (including documentation), and stores each file's revision history.

c. A variety of information is available on GitHub about users and their repositories. Public user profiles can include username, repositories that the user has started, other GitHub users the user follows, and those that follow the user. A user may also choose to not share his or her real name, avatar, affiliated company, location, public email address, personal web page, or organizations to which the user belongs.

d. GitHub provides social networking-like functions such as feeds, followers, wikis (using wiki software called Gollum) and a social network graph to display how developers work on their versions of a repository and what version is newest.

e. GitHub can be accessed on GitHub.com, or through GitHub Enterprise on one's own server, or in a private cloud using Amazon Web Services. GitHub Enterprise is similar to GitHub's public service, but is designed for use by large-scale enterprise software development teams where the enterprise wishes to host their repositories behind a corporate firewall.

III. Jurisdiction to Issue the Requested Warrants

9. Pursuant to Title 18, United States Code, Sections 2703(a), (b)(1)(A) & (c)(1)(A), the Government may require a provider of an electronic communications service or a remote computing service, such as Google, Reddit, or GitHub, to disclose all stored content and all non-content records or other information pertaining to a subscriber, by obtaining a warrant issued using the procedures described in the Federal Rules of Criminal Procedure.

10. A search warrant under Section 2703 may be issued by "any district court of the United States (including a magistrate judge of such a court)" that "has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

11. When the Government obtains records under Section 2703 pursuant to a search warrant, the Government is not required to notify the subscriber of the existence of the warrant. 18 U.S.C. § 2703(a), (b)(1)(A) & (3). Additionally, the Government may obtain an order precluding the Provider from notifying the subscriber or any other person of the warrant, for such period as the Court deems appropriate, where there is reason to believe that such notification will seriously jeopardize an investigation. 18 U.S.C. § 2705(b).

IV. The Subject Offenses

12. For the reasons detailed below, I believe that there is probable cause to believe that the Target Accounts contain evidence, fruits, and instrumentalities of (i) the unauthorized possession and, *inter alia*, the communication of national defense information to someone not entitled to receive it, in violation of Title 18, United States Code, Section 793(d); (ii) the unlawful retention of national defense information, in violation of Title 18, United States Code, Section 793(e); (iii) exceeding authorized access to a computer in order to obtain national defense information with reason to believe that information could be used to the injury of the

United States and the advantage of a foreign nation and willfully transmitting that information to a person not entitled to receive it, in violation of Title 18, United States Code, Section 1030(a)(1); and (iv) intentionally exceeding authorized access to a computer and thereby obtaining information from a department or agency of the United States, in violation of Title 18, United States Code, Section 1030(a)(2)(B) (collectively the "Subject Offenses").

V. Probable Cause

A. WikiLeaks Publication of Classified CIA Information

13. Based on my review of publicly available material on the Internet, including on the website wikileaks.org ("WikiLeaks"), I know that, on March 7, 2017, WikiLeaks published what it claimed were more than 8,000 documents and files that contained classified information (the "Classified Information") belonging to the Central Intelligence Agency ("CIA"). In its press release accompanying the Classified Information, WikiLeaks further claimed that:

a. The public dissemination of the Classified Information was "the largest ever" unauthorized publication of classified CIA documents.

b. The Classified Information constituted the "first full part" of a series—thus indicating that there would be subsequent publications of additional sensitive CIA information.

c. The "collection" obtained by WikiLeaks amounted to "more than several hundred million lines of code" and revealed the "entire hacking capacity" of the CIA, including various malware, viruses, and other tools used by the CIA.

14. Based on my conversations with other law enforcement agents and others, my review of documents, and my training and experience, I know that:

a. The information that WikiLeaks claimed was classified CIA information—that is, the Classified Information—was at the time of its disclosure, in fact,

classified CIA information.

b. Specifically, the Classified Information was created and maintained by one specific group within the CIA which is responsible for various computer engineering activities, including the development of computer code (the "CIA Group"). That CIA Group exists within a larger CIA component (the "CIA Component"). In March 2016, less than 200 employees were assigned to the CIA Group. And only employees of the CIA Group had access to the computer network on which the Classified Information that was stolen from the CIA Group's computer network was stored. (Moreover, as described in detail below, only three of those approximately 200 people who worked for the CIA Group had access to the specific portion of the Group's computer network on which the Classified Information was likely stored.)

c. The Classified Information appears to have been stolen from the CIA Component sometime between the night of March 7, 2016 and the night of March 8, 2016.

i. This is based on preliminary analysis of the timestamps associated with the Classified Information which indicates that March 7, 2016 was the latest (or most recent) creation or modification date associated with the Classified Information.

ii. Because, for the reasons described below (see *infra*), the Classified Information was apparently copied from an automated daily back-up file, it is likely that the Classified Information was copied either late on March 7, 2016 (after the March 7 nightly back-up was completed) or on March 8, 2016 (before the March 8 nightly back-up was completed).

iii. This is so because if the Classified Information was copied before the March 7 back-up, one would not expect to see in the Classified Information documents dated as late as March 7. And if the Classified Information was copied after the March 8 back-up, one would expect to see documents dated on or after March 8 because the "back-ups" occur

approximately each day.¹

d. The Classified Information was publicly released by WikiLeaks exactly one year to the day (March 7, 2017) from the latest date associated with the Classified Information (March 7, 2016).

e. The duplication and removal from the CIA Group's computer network of the Classified Information and its subsequent public dissemination via WikiLeaks was not authorized by the United States government.

f. The unauthorized disclosure of the Classified Information could—at a minimum—reasonably be expected to cause serious damage to the national security of the United States. See Executive Order 13526; 18 C.F.R. § 3a.11(a)(2).

g. The Classified Information is national defense information and its disclosure could reasonably be expected to be used to the injury to the United States and to the advantage of a foreign nation. See 18 U.S.C. § 793(d) & (e).

B. The CIA Group's Local Area Computer Network (LAN) and Back-Up Server

15. Based on my conversations with other law enforcement agents and others, my review of documents, and my training and experience, I know that the Classified Information originated

¹ It is of course possible that the Classified Information was copied later than March 8, 2016 even though the creation/modification dates associated with it appear to end on March 7, 2016. For example, the individual who copied and removed the data could have limited his or her copying to data that was modified or created on or before March 7, 2016. (Conversely, however, the Classified Information is unlikely to have been copied before March 7, 2016, because it contains data that was created as recently as March 7, 2016.) Because the most recent timestamp on the Classified Information reflects a date of March 7, 2016, preliminary analysis indicates that the Classified Information was likely copied between the end of the day on March 7 and the end of the day on March 8.

in a specific isolated local area computer network ("LAN") used exclusively by the CIA Group. As described above, in and around March 2016, in total less than 200 people had access to the CIA Group's LAN on which the Classified Information was stored.

a. An isolated network, such as the CIA Group's LAN, is a network-security structure by which the isolated network is physically separated (or "air-gapped") from unsecured networks, such as the public Internet.

b. Accordingly, such isolated networks, like the LAN, cannot be accessed from the public Internet, but rather only through those computers which are physically connected to the isolated network.

c. The CIA Group's LAN, and each of its component parts, was maintained in heavily physically secured governmental facilities, which include multiple access controls and various other security measures.

d. The isolated LAN used by the CIA Group was comprised of multiple networked computers and servers. (Each of these component computers and servers were, by definition, inside the electronically isolated LAN.)

i. In order to preserve and protect the CIA Group employees' day-to-day computer engineering work, that work was backed up, on an approximately daily basis, to another server on the CIA Group's LAN that was used to store back-up data (the "Back-Up Server").

ii. Back-ups of the sort stored on the Back-Up Server are designed to ensure that, should the original data be corrupted or deleted, the stored data is not lost, but rather—because of the daily back-ups—is maintained via the daily copies stored on the Back-Up

² In its press release announcing the publication of the Classified Information, WikiLeaks stated that the Classified Information originated from "an isolated, high-security network."

Server.

C. The Publicly Disclosed Classified Information Likely Originated on the CIA Group's Back-Up Server

16. Based on my conversations with other law enforcement agents and others, my review of documents, and my training and experience, I understand that the Classified Information that was publicly released by WikiLeaks appears likely to have been copied—specifically—from the CIA Group's Back-Up Server.

a. As described above, the Back-Up Server served as a secondary storage location for data that principally resided on the primary computer network used for CIA Group employees' day-to-day work writing computer code. Approximately each day, an automated process would back-up that data to the Back-Up Server. Each of those daily back-ups was akin to an electronic "snapshot" of the data on that particular date. In that way, the Back-Up Server simultaneously acquired and stored, on a rolling basis, daily snapshots of the original data.

b. As such, if the data contained on the Back-Up Server was copied *en masse* directly from that Server, the copy would contain numerous iterations (or snapshots) of the similar or same data which had been backed up from the original data, distinguished by date.

c. The publicly released Classified Information does, in fact, contain numerous iterations (or snapshots) of the similar or same data, distinguished by date.

d. Accordingly, the fact that the Classified Information contains numerous iterations (or snapshots) of the similar or same data, distinguished by date, is strongly supportive of the fact that the Classified Information was taken from the CIA Group's Back-Up Server.

³ I understand, based on my conversations with others familiar with the CIA Group's LAN that it would be difficult, if not impossible, to copy from the data (not on the Back-Up Server) the multiple different date-distinguished iterations of the same data that are included in the publicly released Classified Information. In contrast, a single copy of the Back-Up Server

c. As described above, because the most recent timestamp associated with the Classified Information appears to be March 7, 2016, it is likely that the Classified Information was copied from the Back-Up Server after the daily back up on March 7, 2016, and before the daily back-up on March 8, 2016.

D. TARGET SUBJECT JOSHUA ADAM SCHULTE Was One of Only Three Employees Across the Entire CIA Who, in March 2016, Had Been Given System Administrator Access to the Back-Up Server

17. Based on my conversations with other law enforcement agents and others, my review of documents, and my training and experience, I know that the CIA Group's LAN was designed such that only those employees who were specifically given a particular type of systems administrator access ("Systems Administrators") could access the Back-Up Server.

a. Systems Administrators were given a particular username and password in order to log on to and access the Back-Up Server.

b. Conversely, CIA employees who were not designated Systems Administrators were not given access to the Back-Up Server.⁴

18. I know, based on my conversations with other law enforcement agents and others, in approximately March 2016—the month when the Classified Information is assessed to have been copied—only three CIA employees were designated Systems Administrators with access to the CIA Group's Back-Up Server.

would likely include each of the prior iterations (or snapshots) of the same data—which is exactly what is reflected in the publicly released Classified Information.

⁴ It is, of course, possible that an employee who was not a designated Systems Administrator could find a way to gain access to the Back-Up Server. For example, such an employee could steal and use—without legitimate authorization—the username and password of a designated Systems Administrator. Or an employee lacking Systems Administrator access could, at least theoretically, gain access to the Back-Up Server by finding a "back-door" into the Back-Up Server.

a. TARGET SUBJECT JOSHUA ADAM SCHULTE ("SCHULTE") was one of those three Systems Administrators.

i. SCHULTE was employed as a computer engineer by the CIA—specifically in the CIA Group—from in or about May 2010 through on or about November 10, 2016, when he resigned from the CIA.

ii. During SCHULTE's more than six years working in the CIA Group, his responsibilities included, among other things, developing computer code for specific projects, including projects explicitly described in the Classified Information.

iii. SCHULTE had a skill set that enabled him to write computer code designed to clandestinely copy data from computers.

b. As described above, in March 2016, SCHULTE was one of only three CIA employees throughout the entire CIA who had authorized access to the CIA Group's Back-Up Server from which the Classified Information was likely copied. The publicly released Classified Information published by WikiLeaks, based on a preliminary review, appears to contain the names and/or pseudonyms of, *inter alia*, multiple CIA employees—including two of the three aforementioned individuals with designated Systems Administrator privileges.

i. Names used by the other two CIA Group Systems Administrators were, in fact, published in the publicly released Classified Information.

ii. SCHULTE's name, on the other hand, was not apparently published in the Classified Information.

iii. Thus, SCHULTE was the only one of the three Systems Administrators with access to the Classified Information on the Back-Up Server who was not publicly identified via WikiLeaks's publication of the Classified Information.

c. The other two individuals who served in March 2016 as Systems Administrators for the CIA Group's LAN remain employed by the CIA. SCHULTE resigned from the CIA in November 2016, as described in detail below.

II. SCHULTE Had Access to the Back-Up Server on March 7 and 8, 2016—The Likely Dates of the Copying of the Classified Information

19. As described above, it appears likely that the Classified Information was copied between March 7 and March 8, 2016.

a. Based on my conversations with other law enforcement agents and others, and my review of documents, including access records of the CIA Component facility in which SCHULTE worked, I know that he was present at work from approximately:

- i. 10:01 a.m. until 7:16 p.m. on March 7, 2016; and
- ii. 10:19 a.m. until 7:40 p.m. on March 8, 2016.

b. Based on my conversations with other law enforcement agents and others, and my review of documents, I know that on March 8, 2016, the CIA Group held an offsite management retreat for many of its senior and midlevel managers. Accordingly, on March 8th, much of the CIA Group's management, including some to whom SCHULTE reported, were not present in the CIA Component building where SCHULTE and other CIA Group employees worked.

c. I further understand that SCHULTE's workspace (i.e., his desk and computer workstation) was set up such that only three other CIA Group Employees had direct line-of-sight to SCHULTE's desk and computer—that is, only three other employees could see what he was doing at his desk. At least two of those three employees were at the offsite management retreat on March 8, 2016.

d. As described above, in March 2016, only two CIA employees in addition

to SCHULTE were designated Systems Administrators with access to the CIA Group's Back-Up Server from which the Classified Information was likely copied. On March 8, 2016, one of those two other designated Systems Administrators was at the offsite management retreat. (The retreat was held at a location that did not have any access to the CIA Group's LAN, including the Back-up Server, and therefore afforded no access to the Classified Information.)⁵

F. SCHULTE's Unauthorized Unilateral Reinstatement of His Own Administrative Privileges

20. Based on my conversations with other law enforcement agents and others, and my review of documents, I understand that, on or about April 4, 2016, around the time of his reassignment to another branch within the CIA Group, many of SCHULTE's administrator privileges on the LAN were revoked, and he was no longer permitted to serve as a Systems Administrator in the CIA Group's LAN.

a. At the same time, on or about April 4, 2016, SCHULTE's computer access to a specific developmental project ("Project-1") was also revoked. Until his reassignment, SCHULTE had been the CIA Group employee with principal responsibility for Project-1.

b. Upon that transfer, principal responsibility for Project-1 was transferred to another CIA Group employee, who received computer access to Project-1.⁶

c. I know from my review of publicly available material on the Internet, including WikiLeaks.org, that Project-1 was one of a small group of CIA projects and

⁵ On March 7 and 8, 2016, the third of the three CIA employees with Systems Administrator access was located at a CIA facility that did, in fact, have access to the Back-Up Server from which the Classified Information was likely copied.

⁶ SCHULTE retained read-only access to Project-1 (but not the ability to alter the code) and the ability to copy the computer code associated with it in order to support another project for which he had responsibility.

capabilities that WikiLeaks highlighted explicitly by name in its March 7, 2017 press release that accompanied the online publication of the Classified Information.

21. Based on my conversations with other law enforcement agents and others, and my review of documents, I understand that, less than two weeks later, on or about April 11, 2016, SCHULTE unilaterally, and without authorization, logged onto the CIA Group's LAN and reinstated his own administrator privileges.

a. On or about April 14, 2016, CIA Group management discovered that SCHULTE had personally re-instituted his administrator privileges without permission.

b. On or about April 18, 2016, SCHULTE received notice regarding CIA policies against personnel restoring their own access to privileges or computer networks after those accesses have been revoked. SCHULTE signed an acknowledgment that he understood that "Individuals are not permitted to personally attempt and/or renew their previous authorizations [including administrator privileges] to any particular [computer] system." That notice further instructed SCHULTE: "do not attempt to restore or provide yourself administrative rights to any project and/or system for which they have been removed."

c. A little more than one month later, on May 26, 2016, and notwithstanding the warnings described above, SCHULTE made an official request that he again be given full access to Project-1. Before receiving a response to that request, SCHULTE requested access from another employee who, apparently without proper vetting, granted SCHULTE the requested full access to Project-1.

i. On the same day, SCHULTE used that newly obtained access to, unilaterally and without authorization, revoke the computer access permissions of all other CIA Group employees to work on Project-1.

ii. Once this conduct was discovered, SCHULTE was issued a letter of warning that stated, "You were aware of the policy for access and your management's lack of support for you to retain administrative privileges, but nonetheless you took steps to deliberately violate that policy and gain those privileges." It continued by warning SCHULTE that any future violations would result in "further administrative action of a more severe nature."

iii. After receiving the letter of warning, SCHULTE disagreed with some of its conclusions and consequently refused to sign the form.

22. Based on my conversations with other law enforcement agents and others, my review of documents, and my training and experience, I know that SCHULTE's accessing of information on the LAN that he had been expressly forbidden by the CIA to access, and his accessing of information which he had been electronically prevented from accessing by the CIA, using a computer network on which he was permitted to access other, distinct information, exceeded his authorized access to the government-owned and controlled computer networks of the CIA. See 18 U.S.C. § 1030(a)(1) & (a)(2)(B).

G. Internal CIA Investigation of SCHULTE and a CIA Colleague

23. Based on my conversations with other law enforcement agents and others, my review of documents, and my training and experience, I know that, in or around March 2016, SCHULTE came to the attention of CIA security after SCHULTE alleged that another CIA Group co-worker had made a threat against him. SCHULTE expressed deep unhappiness about the way that CIA responded to the alleged threat. He threatened legal action against the CIA for its handling of the situation, and repeatedly stated that he felt that he was being punished by CIA management for reporting the alleged threat incident. SCHULTE informed CIA security that, if "forced into a corner" he would proceed with a lawsuit against the CIA. He also repeatedly threatened that he or his lawyer would go to the media. In addition, CIA security learned that

SCHULTE had removed an internal CIA document from CIA facilities that regarded his complaints to the CIA concerning its handling of the alleged threat, despite being told multiple times by CIA security officials not to do so.

24. In approximately August 2016, as part of a standard background reinvestigation of SCHULTE for the purpose of renewing his security clearances, the CIA conducted interviews of multiple CIA Group colleagues. Among other things:

a. Some (but not all) colleagues independently reported that SCHULTE's demeanor with his management and colleagues, and his commitment to his work, changed markedly for the worse in or around February 2016.

b. Multiple colleagues stated that SCHULTE had indicated that he felt aggrieved by the CIA in a number of respects. Some also reported that they believed SCHULTE to be untrustworthy and potentially subject to outside coercion. (Other colleagues made no such report and, indeed affirmatively reported that they believed that SCHULTE was, in fact, trustworthy.)

c. Some (but not all) colleagues also reported that SCHULTE's security practices were lax, and that SCHULTE tended not to abide by security guidelines he deemed inconvenient—particularly guidelines concerning when and what kinds of media or data (such as external drives) could be connected or uploaded to CIA computer systems.⁷

H. SCHULTE's November 2016 Resignation from the CIA

25. Based on my conversations with other law enforcement agents and others, my review of documents, and my training and experience, I know that, in connection with and preceding SCHULTE's November 2016 resignation from the CIA, he sent the following communications,

⁷ External drives can be connected to computers and files in order to allow users to move files from the computers onto the portable external drives.

among others:

a. Approximately one month prior to his resignation, on October 12, 2016, SCHULTE, using his CIA email account, sent an email to another CIA Group employee at that employee's official email account. The subject line of the email stated, "ROUGH DRAFT of Resignation Letter *BYPASS ONLY*." The email contained a letter entitled "Letter of Resignation 10/12/16" and addressed to "To whomever it may concern" ("Draft Resignation Letter"). I know from reviewing the Draft Resignation Letter, which spanned approximately three single-spaced pages, the following:

i. SCHULTE began the letter by stating, in substance and in part, that he had "always been a patriot" and would "obviously continue to support and defend this country until the day that I die," but that "from this day forward" he would "no longer do so as a public servant."

ii. SCHULTE claimed that he believed that the CIA Group management had unfairly "velled" CIA leadership from various of SCHULTE's previously expressed concerns, including concerns about the network security of the CIA Group's LAN. SCHULTE continued: "That ends now. From this moment forward you can no longer claim ignorance; you can no longer pretend that you were not involved."

iii. SCHULTE explained that he was resigning from the CIA because CIA Group management had, among other things, "ignored" issues he had raised about "security concerns" and had attempted to "conceal these practices from senior leadership," including that the CIA Group's LAN was "incredibly vulnerable" to the theft of sensitive data. He claimed that one named CIA Group manager had ignored his security concerns and "later attempt[ed] to evade responsibility and blame the decentralized and insecure [CIA Group computing]

environment entirely on me.”⁸

iv. Specifically, SCHULTE wrote that inadequate CIA security measures had “left [the CIA Group’s LAN] open and easy for anyone to gain access and easily download [from the LAN] and upload [sensitive CIA Group computer code] in its entirety to the [public] internet.”

b. It appears that SCHULTE did not, in fact, submit the Draft Resignation Letter.

c. On his last day with the CIA (November 10, 2016), SCHULTE did, however, send an internal email to the CIA Office of the Inspector General (OIG) advising that office that he had been in contact with the United States House of Representatives’ Permanent Select Committee on Intelligence regarding his complaints about the CIA (“OIG Email”).

i. In the OIG Email, which SCHULTE labeled “Unclassified,” SCHULTE raised many of the same complaints included in the draft “Letter of Resignation 10/12/16,” described above, including the CIA’s treatment of him and its failure to address the “security concerns” he had repeatedly raised in the past.

ii. Shortly thereafter, CIA security learned that one of SCHULTE’s colleagues had witnessed SCHULTE printing the OIG Email, placing it in a folder, and exiting the CIA Component facility where SCHULTE worked.

iii. Notwithstanding SCHULTE’s labeling of the email as “Unclassified,” the CIA subsequently determined that the OIG Email which SCHULTE removed from the CIA without authorization did, in fact, contain classified information.

⁸ SCHULTE went on to describe other complaints he had about managers at the CIA. Among other things, SCHULTE described his complaints about the way in which CIA Group management had handled various personnel and disciplinary issues (*see supra* at Part II.G.16).

I. SCHULTE's Use Of the Subject Google Account To Make Inquiries About the Status of the Investigation

26. Based on my conversations with other law enforcement agents and others, and my review of documents, I understand that, since the March 7, 2017 publication of the Classified Information on WikiLeaks, SCHULTE has repeatedly initiated contact, via telephone and text messages, with multiple of his former CIA Group colleagues. Those colleagues have reported that contact to government and law enforcement officials.

a. In those communications with his former colleagues, SCHULTE has repeatedly asked about the status of the investigation into the disclosure of the Classified Information.

b. SCHULTE has requested more details on the information that was disclosed.

c. SCHULTE has inquired of his interlocutors' personal opinions regarding who, within the CIA Group, each believes is responsible for the disclosure of the Classified Information. SCHULTE has also asked what other former CIA Group colleagues are saying about the disclosure.

d. SCHULTE has repeatedly denied any involvement in the disclosure of the Classified Information.

e. SCHULTE has indicated that he believes that he is a suspect in the investigation of the leak of Classified Information.

f. I am not aware of any other former CIA employee who has initiated any contact with former colleagues regarding the disclosure of the Classified Information.

27. Furthermore, I know that SCHULTE has specifically used the Subject Google Account, *i.e.*, the account associated with the Gmail account joashulte1@gmail.com, to make

some of the inquiries described above. For example:

a. Records show that, on or about March 7, 2017, when WikiLeaks released the Classified Information, SCHULTZ used the Google Voice feature associated with the Subject Google Account to send approximately 149 texts to multiple of his former colleagues at the CIA.

b. SCHULTZ, using the Google Voice feature associated with the Subject Google Account, also had phone calls with former CIA colleagues, including one telephone call with a former colleague in which he, among other things, inquired of the former colleague's personal opinions regarding who was responsible for the disclosure of the Classified Information and what the person's motivation might be. SCHULTZ indicated that he believed that the person responsible was a contractor who disclosed the Classified Information for fame.

c. In a call using the telephone number associated with the Subject Google Account on March 8, 2017 with the same former colleague, SCHULTZ denied his involvement in the disclosure of the Classified Information, indicated his belief that many people suspected him of the disclosure, and relayed a conversation with another acquaintance in which SCHULTZ had denied involvement in the disclosure of the Classified Information, but was dissatisfied with the acquaintance's reaction to SCHULTZ's denial.

d. Records for recent communications on the Gmail feature of the Subject Google Account show that SCHULTZ also continues to use various Google Services to communicate with others, including his Gmail address joshachultz1@gmail.com, which is listed as the recipient facility for several messages SCHULTZ has received in the past two days. As discussed above, SCHULTZ's account also reflects as recently as this month his enrollment in other Google Services, including Android, Google Docs, Google Drive, Google Groups, Google

Calendar, Google Hangouts, Google Payments, Google Photos, Google+, and Google Code.

J. The Subject Reddit Account and the Subject GitHub Account

28. Based on my conversations with other law enforcement agents and others, and my review of documents, I also know that references to SCHULTE in the context of the release of the Classified Information have been made on other websites, including those hosted by Reddit and GitHub. Specifically:

a. On or about March 7, 2017—i.e., the date of the release of the Classified Information by WikiLeaks—a “thread,” or online discussion, was opened by a Reddit user which was devoted to the release of the Classified Information.

b. As part of the thread, the user of the Subject Reddit Account made a post that stated: “What about this guy pedbsktbl?” (with the word “pedbsktbl” highlighted). The comment was followed by, among other things, (1) a listing of the following website: <https://github.com/pedbsktbl/projectwizard/blob/master/ProjectWizard/tempSubmodule.xml> (the “Website”) and (2) a line of text stating, “pedbsktbl - > Joshua Schulte.”

c. I know, based on a review of publicly available websites, including those available through various social media sites, that SCHULTE employs the user name “pedbsktbl” on various of these websites. For example, I know from reviewing a posting on the Google+ service associated with the Subject Google Account, which contains a photograph of SCHULTE, that SCHULTE listed various of his other social media accounts, several of which (e.g., including Facebook and Twitter) contain or reference the user name “pedbsktbl.”

29. I also know from viewing the Website, which features a page associated with the Subject GitHub Account, that the Webpage contains numerous lines of computer code, some of which reference computer applications that were referenced in the information released by WikiLeaks.

30. I respectfully submit that there is probable cause therefore to believe that the Target Accounts contain evidence, fruits, and instrumentalities of the Subject Offenses. Among other things, I respectfully submit that there is probable cause to establish that SCHULTZ is proficient in and makes use of Internet-based computing services, like those offered by the Providers through the Target Accounts. Moreover, based on my training and experience, I know that individuals who engage in the Subject Offenses often use Internet-based services (like the Target Accounts) as a means by which to communicate with co-conspirators as well as means through which not only to transmit but also to store purloined information so that they do not have to carry it on their person. Finally, I know that individuals who engage in the Subject Offenses oftentimes use Internet-based computing services, like the Target Accounts, to publish purloined information. For example, based on my training and experience and my involvement in this investigation, I know that WikiLeaks is an Internet-based publication and that individuals who provide information to WikiLeaks in the past oftentimes have done so through the use of other Internet-based computing platforms, like the Target Accounts and other services offered by the Providers. Accordingly, when each of these factors is considered in conjunction with the fact of SCHULTZ's access to the purloined information, his clear proficiency in computers and computer-programming, and the probable cause establishing SCHULTZ's access to and use of the Subject Accounts, I respectfully submit that there is probable cause to believe that the Subject Accounts will contain evidence, fruits, and instrumentalities of the Subject Offenses.

K. SCHULTZ's Planned Travel

31. Based on my conversations with other law enforcement agents and others, and my review of documents, including information provided by the Department of Homeland Security, I understand that SCHULTZ has booked an international flight departing on Thursday, March 16, 2017. (Return travel to the United States is booked for a few days later.) The

aforementioned records and conversations reflect that this is only SCHULTZ's second trip reflected in DHS records outside the United States.

VI. Evidence, Fruits and Instrumentalities in Target Accounts

32. Based upon the foregoing, I respectfully submit there is probable cause to believe that information stored on the Providers' servers associated with the Target Accounts will contain evidence, fruits, and instrumentalities of the Subject Offenses, as more fully described in Section II of Attachment A to the requested warrants.

33. In particular, I believe the Target Accounts are likely to contain, among other things, the following information:

- a. Evidence of the identity(s) of the user(s) of the Target Accounts as well as other coconspirators in contact with the Target Accounts;
- b. Evidence relating to the participation in the Subject Offenses by the users of the Target Accounts and others, including information relating to the unauthorized retention, gathering, and transmission of classified documents or materials, and the unauthorized removal and retention of classified documents or materials;
- c. Communications evidencing crimes, including but not limited to correspondence with others relating to the unauthorized retention, gathering, and transmission of classified documents or materials, and the unauthorized removal and retention of classified documents or materials;
- d. Items, records or information consisting of, referring to, or reflecting classified documents or materials on the Target Accounts;
- e. Evidence concerning financial institutions and transactions used by the users of the Target Accounts in furtherance of the Subject Offenses;

- f. Evidence of and relating to computers or other online accounts and facilities (such as additional email addresses) controlled or maintained by the user of the Target Accounts;
- g. Passwords or other information needed to access any such computers, accounts, or facilities; and
- h. With respect to the Subject Google Account, evidence relating to the geolocation and travel of the user(s) of the Target Accounts at times relevant to the Subject Offenses.

34. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for service of a search warrant issued under § 2703, or for the collection or production of responsive records. Accordingly, the warrants requested herein will be transmitted to the Providers, which will be directed to produce a digital copy of any responsive records to law enforcement personnel within 10 days from the date of service. Law enforcement personnel (including, in addition to law enforcement officers and agents, and depending on the nature of the BSI and the status of the investigation and related proceedings, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) will retain the records and review them for evidence, fruits, and instrumentalities of the Subject Offenses as specified in Section III of Attachment A to the requested warrants, which shall not be transmitted to the Providers.

35. In conducting this review, law enforcement personnel may use various methods to locate evidence, fruits, and instrumentalities of the Subject Offenses, including but not limited to undertaking a cursory inspection of all content associated with the Target Accounts. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine

which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, to the extent applicable, including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with emails, including attachments such as scanned documents, pictures, and videos, do not store data as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications in an account, as it is impossible to know in advance all of the unique words or phrases that investigative subjects will use in their communications, and consequently there are often many communications in an account that are relevant to an investigation but that do not contain any keywords that an agent is likely to search for.

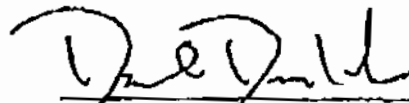
VII. Request for Non-Disclosure and Sealing Orders

36. The existence and scope of this ongoing criminal investigation are not publicly known. As a result, premature public disclosure of this affidavit or the requested warrants could alert potential criminal targets that they are under investigation, causing them to destroy evidence, flee from prosecution, or otherwise seriously jeopardize the investigation. In particular, given that targets of the investigation are known to use computers and electronic communications in furtherance of their activity, the targets could easily delete, encrypt, or otherwise conceal such digital evidence from law enforcement were they to learn of the Government's investigation.

37. Accordingly, there is reason to believe that, were the Providers to notify the subscriber(s) or others of the existence of the requested warrants, the investigation would be seriously jeopardized. Pursuant to 18 U.S.C. § 2705(b), I therefore respectfully request that the

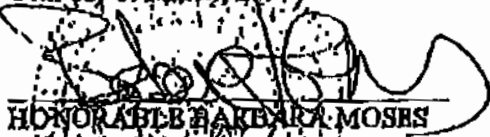
Court direct the Providers not to notify any person of the existence of the warrant for a period of 180 days from issuance, subject to extension upon application to the Court, if necessary.

38. For similar reasons, I respectfully request that this affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise, except that the Government be permitted without further order of this Court to provide copies of the warrant and affidavit as need be to personnel assisting it in the investigation and prosecution of this matter, and to disclose those materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.



Special Agent Jeff D. Donaldson
Federal Bureau of Investigation

Sworn to before me this
14th day of March, 2017.



HONORABLE BARBARA MOSES
United States Magistrate Judge
Southern District of New York

17 MAG 6861

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK**

In the Matter of a Warrant for All
Content and Other Information for the
Google account associated with Email
Address joshschulte@gmail.com,
Maintained at Premises Controlled by
Google, Inc. and Google Payment
Corp.

SEARCH WARRANT AND NON-DISCLOSURE ORDER

TO: Google, Inc. and Google Payment Corp. ("Google")

The Federal Bureau of Investigation (the "FBI" or the "Investigative Agency")

1. Warrant. Upon an affidavit of Special Agent of the FBI and pursuant to the provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) and § 2703(e)(1)(A), and the relevant provisions of Federal Rule of Criminal Procedure 41, the Court hereby finds that there is probable cause to believe that content information maintained at premises controlled by Google associated with the email address joshschulte@gmail.com contains evidence, fruits, and instrumentalities of a crime, all as specified in Attachment A hereto. Accordingly, Google is hereby directed to provide to the Investigative Agency, within 10 days of the date of service of this Warrant and Order, the records specified in Section II of Attachment A hereto, for subsequent review by law enforcement personnel as authorized in Section III of Attachment A, which shall not be transmitted to the Provider. The Government is required to serve a copy of this Warrant and Order on Google within 14 days of the date of issuance. The Warrant and Order may be served via electronic transmission or any other means through which Google is capable of accepting service.

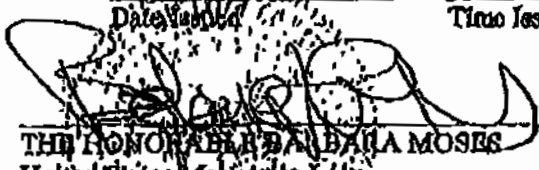
USG-CONFIDENTIAL

JAS_000128

2. **Non-Disclosure Order.** Pursuant to 18 U.S.C. § 2705(b), the Court finds that there is reason to believe that notification of the existence of this warrant will result in destruction of or tampering with evidence, danger to the physical safety of an individual, flight from prosecution, and/or intimidation of potential witnesses or otherwise will seriously jeopardize an ongoing investigation. Accordingly, it is hereby ordered that Google shall not disclose the existence of this Warrant and Order to the listed subscriber or to any other person for a period of 180 days from the date of this Order, subject to extension upon application to the Court if necessary, except that Google may disclose this Warrant and Order to an attorney for Google for the purpose of receiving legal advice.

3. **Sealing.** It is further ordered that this Warrant and Order, and the Affidavit upon which it was issued, be filed under seal, except that the Government may without further order of this Court serve the Warrant and Order on Google; provide copies of the Affidavit or Warrant and Order as need be to personnel assisting the Government in the investigation and prosecution of this matter; and disclose these materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

Dated: New York, New York

3/14/17 1:11 AM
 Date Issued Time Issued

 THE HONORABLE DALIA MOSES
 United States Magistrate Judge
 Southern District of New York

Attachment A

I. The Subject Account and Execution of Warrant

This warrant is directed to Google, Inc. and Google Payment Corp. (collectively, "Google" or the "Provider") and applies to all content and other information within Google's possession, custody, or control that is associated with the email address `joshschulte1@gmail.com` (the "Subject Gmail Account").

A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to Google. Google is directed to produce to the law enforcement officer an electronic copy of the information specified in Section II below. Upon receipt of the production, law enforcement personnel will review the information for items falling within the categories specified in Section III below, a copy of which shall not be transmitted to the Provider.

II. Information to be Produced by Google

To the extent it is within Google's possession, custody, or control, Google is directed to produce the following information associated with the Subject Gmail Account:

a. Search History. All data concerning searches run by the user of the Subject Gmail Accounts, including, but not limited to, the content, date, and time of the search.

b. Google+ Photos and Content. All data concerning Google+ Photos, including all albums, photos, videos, and associated metadata for each file, as well as all Google+ posts, comments, profiles, contacts, and information relating to Google+ Circles.

c. Google Drive Content. All files and folders in the Google Drive associated with the Subject Gmail Account.

d. Google Voice. All records, voicemails, text messages, and other data associated with Google Voice.

USG-CONFIDENTIAL

JAS_000128

e.

f. *Google Wallet Content.* All data and information in the Google Wallet associated with the Subject Gmail Account.

g. *YouTube Content.* For any YouTube account associated with the Subject Gmail Account, all subscriber information as well as copies of any videos and associated metadata and any YouTube comments or private messages.

h. *Android Content.* Any Android device information associated with the Subject Gmail Account, including IMEI/MBID, make and model, serial number, date and IP of last access to Google, and a list of all accounts that have ever been active on the device.

i. *Email Content.* All emails sent to or from, stored in draft form in, or otherwise associated with the Subject Gmail Account, including all message content, attachments, and header information (specifically including the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email).

j. *Address book information.* All address book, contact list, or similar information associated with the Subject Gmail Account.

k. *Subscriber and payment information.* All subscriber and payment information regarding the Subject Gmail Account, including but not limited to name, username, address, telephone number, alternate email addresses, registration IP address, account creation date, account status, length of service, types of services utilized, means and source of payment, and payment history.

l. *Linked accounts.* The account identifiers for all accounts linked to the Subject Gmail Accounts, and subscriber records therefore as described in the preceding sub-paragraph,

including but not limited to any account linked to the Subject Gmail Account by registration IP address, "machine" or other cookie, alternate email address, or telephone number.

m. Transactional records. All transactional records associated with the Subject Gmail Account, including any IP logs or other records of session times and durations.

n. Customer correspondence. All correspondence with the subscriber or others associated with the Subject Gmail Account, including complaints, inquiries, or other contacts with support services and records of actions taken.

o. Preserved records. Any preserved copies of any of the foregoing categories of records created in response to any preservation request(s) issued pursuant to 18 U.S.C. § 2703(f).

III. Review of Information by the Government

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by Google in order to locate any evidence, fruits, and instrumentalities of violations (i) the unauthorized possession and, *inter alia*, the communication of national defense information to someone not entitled to receive it, in violation of Title 18, United States Code, Section 793(d); (ii) the unlawful retention of national defense information, in violation of Title 18, United States Code, Section 793(e); (iii) exceeding authorized access to a computer in order to obtain national defense information with reason to believe that information could be used to the injury of the United States and the advantage of a foreign nation and willfully transmitting that information to a person not entitled to receive it, in violation of Title 18, United States Code, Section 1030(a)(1); and (iv) intentionally exceeding authorized access to a computer and thereby obtaining information from a department or agency of the United States,

In violation of Title 18, United States Code, Section 1030(a)(2)(B) (collectively the "Subject Offenses"), including the following:

- i. Evidence of the identity(s) of the user(s) of the Subject Gmail Account as well as other coconspirators in contact with the Subject Gmail Account;
- j. Evidence relating to the geolocation and travel of the user(s) of the Subject Gmail Account at times relevant to the Subject Offenses;
- k. Evidence relating to the participation in the Subject Offenses by the users of the Subject Gmail Account and others;
- l. Evidence concerning financial institutions and transactions used by the users of the Subject Gmail Account in furtherance of the Subject Offenses;
- m. Communications evidencing crimes, including but not limited to correspondence with others relating to the unauthorized retention, gathering, and transmission of classified documents or materials, and the unauthorized removal and retention of classified documents or materials;
- n. Evidence of and relating to computers or other online accounts and facilities (such as additional email addresses) controlled or maintained by the user of the Subject Gmail Account; and
- o. Passwords or other information needed to access any such computers, accounts, or facilities.

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

17 MAG 6961

In the Matter of a Warrant for All
Content and Other Information for the
Reddit, Inc. account associated with
account name L1347517, Maintained
at Premises Controlled by Reddit, Inc.

SEARCH WARRANT AND NON-DISCLOSURE ORDER

TO: Reddit, Inc.

The Federal Bureau of Investigation (the "FBI" or the "Investigative Agency")

1. **Warrant.** Upon an affidavit of Special Agent of the FBI and pursuant to the provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) and § 2703(o)(1)(A), and the relevant provisions of Federal Rule of Criminal Procedure 41, the Court hereby finds that there is probable cause to believe that content information maintained at premises controlled by Reddit, Inc. associated with account name L1347517 contains evidence, fruits, and instrumentalities of a crime, all as specified in Attachment A hereto. Accordingly, Reddit, Inc. is hereby directed to provide to the Investigative Agency, within 10 days of the date of service of this Warrant and Order, the records specified in Section II of Attachment A hereto, for subsequent review by law enforcement personnel as authorized in Section III of Attachment A, a copy of which shall not be transmitted to the Provider. The Government is required to serve a copy of this Warrant and Order on Reddit, Inc. within 14 days of the date of issuance. The Warrant and Order may be served via electronic transmission or any other means through which Reddit, Inc. is capable of accepting service.

2. **Non-Disclosure Order.** Pursuant to 18 U.S.C. § 2705(b), the Court finds that there is reason to believe that notification of the existence of this warrant will result in destruction of or

tampering with evidence, danger to the physical safety of an individual, flight from prosecution, and/or intimidation of potential witnesses or otherwise will seriously jeopardize an ongoing investigation. Accordingly, it is hereby ordered that Reddit, Inc. shall not disclose the existence of this Warrant and Order to the listed subscriber or to any other person for a period of 180 days from the date of this Order, subject to extension upon application to the Court if necessary, except that Reddit, Inc. may disclose this Warrant and Order to an attorney for Reddit, Inc. for the purpose of receiving legal advice.

3. Sealing. It is further ordered that this Warrant and Order, and the Affidavit upon which it was issued, be filed under seal, except that the Government may without further order of this Court serve the Warrant and Order on Reddit, Inc.; provide copies of the Affidavit or Warrant and Order as need be to personnel assisting the Government in the investigation and prosecution of this matter; and disclose these materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

Dated: New York, New York

2/14/17
Date Issued
1:12 AM
Time Issued
THE HONORABLE BARBARA MOSES
United States Magistrate Judge
Southern District of New York

Attachment A

I. The Subject Account and Execution of Warrant

This warrant is directed to Reddit, Inc. (the "Provider") and applies to all content and other information within Reddit, Inc.'s possession, custody, or control that is associated with the account name L1347517 (the "Subject Account").

A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to Reddit, Inc. Reddit, Inc. is directed to produce to the law enforcement officer an electronic copy of the information specified in Section II below. Upon receipt of the production, law enforcement personnel will review the information for items falling within the categories specified in Section III below, a copy of which shall not be transmitted to the Provider.

II. Information to be Produced by Reddit, Inc.

To the extent it is within Reddit, Inc.'s possession, custody, or control, Reddit, Inc. is directed to produce the following information associated with the Subject Account:

a. Search History. All data concerning searches run, and posts accessed by the user of the Subject Account, including, but not limited to, the content, date, and time of the search or post access.

b. Post Content. All posts and messages made by the Subject Account, including all content, attachments, and any other information (specifically including the date and time at which each post or message was made/sent, and the size and length of each post/message).

c. Email Content or Direct Message Content. All emails and/or direct messages sent to or from, stored in draft form in, or otherwise associated with the Subject Account, including all message content, attachments, and header information (specifically including the source and

USG-CONFIDENTIAL

JAS_000134

destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email).

d. Subscriber and payment information. All subscriber and payment information regarding the Subject Account, including but not limited to name, username, address, telephone number, alternate email addresses, registration IP address, account creation date, account status, length of service, types of services utilized, means and source of payment, and payment history.

e. Transactional records. All transactional records associated with the Subject Account, including any IP logs or other records of session times and durations.

f. Customer correspondence. All correspondence with the subscriber or others associated with the Subject Account, including complaints, inquiries, or other contacts with support services and records of actions taken.

g. Preserved records. Any preserved copies of any of the foregoing categories of records created in response to any preservation request(s) issued pursuant to 18 U.S.C. § 2703(f).

III. Review of Information by the Government

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by Reddit, Inc. in order to locate any evidence, fruits, and instrumentalities of violations (i) the unauthorized possession and, *inter alia*, the communication of national defense information to someone not entitled to receive it, in violation of Title 18, United States Code, Section 793(d); (ii) the unlawful retention of national defense information, in violation of Title 18, United States Code, Section 793(e); (iii) exceeding authorized access to a computer in order to obtain national defense information with reason to

believe that information could be used to the injury of the United States and the advantage of a foreign nation and willfully transmitting that information to a person not entitled to receive it, in violation of Title 18, United States Code, Section 1030(a)(1); and (iv) intentionally exceeding authorized access to a computer and thereby obtaining information from a department or agency of the United States, in violation of Title 18, United States Code, Section 1030(a)(2)(B) (collectively the "Subject Offenses"), including the following:

- p. Evidence of the identity(s) of the user(s) of the Subject Account as well as other coconspirators in contact with the Subject Account;
- q. Evidence relating to the geolocation and travel of the user(s) of the Subject Account at times relevant to the Subject Offenses;
- r. Evidence relating to the participation in the Subject Offenses by the users of the Subject Account and others;
- s. Evidence concerning financial institutions and transactions used by the users of the Subject Account in furtherance of the Subject Offenses;
- t. Communications evidencing crimes, including but not limited to correspondence with others relating to the unauthorized retention, gathering, and transmission of classified documents or materials, and the unauthorized removal and retention of classified documents or materials;
- u. Evidence of and relating to computers or other online accounts and facilities (such as additional email addresses) controlled or maintained by the user of the Subject Account; and
- v. Passwords or other information needed to access any such computers, accounts, or facilities.

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

17 MAG 6961

In the Matter of a Warrant for All
Content and Other Information for the
GitHub account associated with the
user name pedbsktbl, Maintained at
Premises Controlled by GitHub, Inc.

SEARCH WARRANT AND NON-DISCLOSURE ORDER

TO: GitHub, Inc.

The Federal Bureau of Investigation (the "FBI" or the "Investigative Agency")


1. Warrant. Upon an affidavit of Special Agent of the FBI and pursuant to the provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) and § 2703(o)(1)(A), and the relevant provisions of Federal Rule of Criminal Procedure 41, the Court hereby finds that there is probable cause to believe that content (information maintained at premises controlled by GitHub, Inc. associated with the user name pedbsktbl) contains evidence, fruits, and instrumentalities of a crime, all as specified in Attachment A hereto. Accordingly, GitHub, Inc. is hereby directed to provide to the Investigative Agency, within 10 days of the date of service of this Warrant and Order, the records specified in Section II of Attachment A hereto, for subsequent review by law enforcement personnel as authorized in Section III of Attachment A, a copy of which shall not be transmitted to the Provider. The Government is required to serve a copy of this Warrant and Order on GitHub, Inc. within 14 days of the date of issuance. The Warrant and Order may be served via electronic transmission or any other means through which GitHub, Inc. is capable of accepting service.

2. Non-Disclosure Order. Pursuant to 18 U.S.C. § 2705(b), the Court finds that there is reason to believe that notification of the existence of this warrant will result in destruction of or

tampering with evidence, danger to the physical safety of an individual, flight from prosecution, and/or intimidation of potential witnesses or otherwise will seriously jeopardize an ongoing investigation. Accordingly, it is hereby ordered that GitHub, Inc. shall not disclose the existence of this Warrant and Order to the listed subscriber or to any other person for a period of 180 days from the date of this Order, subject to extension upon application to the Court if necessary, except that GitHub, Inc. may disclose this Warrant and Order to an attorney for GitHub, Inc. for the purpose of receiving legal advice.

3. Sealing. It is further ordered that this Warrant and Order, and the Affidavit upon which it was issued, be filed under seal, except that the Government may without further order of this Court serve the Warrant and Order on GitHub, Inc.; provide copies of the Affidavit or Warrant and Order as need be to personnel assisting the Government in the investigation and prosecution of this matter; and disclose these materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

Dated: New York, New York

3/14/17 1:12 A.M.
 Date Issued Time Issued

 THE HONORABLE BARBARA MOSES
 United States Magistrate Judge
 Southern District of New York

Attachment A

I. The Subject Account and Execution of Warrant

This warrant is directed to GitHub, Inc. (the "Provider") and applies to all content and other information within GitHub, Inc.'s possession, custody, or control that is associated with the user name pedbsktbl (the "Subject Account").

A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to GitHub, Inc. GitHub, Inc. is directed to produce to the law enforcement officer an electronic copy of the information specified in Section II below. Upon receipt of the production, law enforcement personnel will review the information for items falling within the categories specified in Section III below, a copy of which shall not be transmitted to the Provider.

II. Information to be Produced by GitHub, Inc.

To the extent it is within GitHub, Inc.'s possession, custody, or control, GitHub, Inc. is directed to produce the following information associated with the Subject Account:

a. Use of GitHub Features. All features used by the Subject Account (e.g., code review, project management, integrations, community management, documentation, code hosting, productivity tools). With respect to each feature used by the Subject Account, provide all data posted by or associated with the Subject Account.

b. GitHub Platforms. All platforms used by the Subject Account (e.g., Atom, Electron, GitHub Desktop). With respect to each platform used by the Subject Account, provide all data posted by or associated with the Subject Account.

c. GitHub Repositories. All data from GitHub repositories that were posted by or associated with the Subject Account.

d. Email Content or Direct Message Content. All emails or direct messages sent to or from, stored in draft form in, or otherwise associated with the Subject Account, including all message content, attachments, and header information (specifically including the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email).

e. Address book information. All address book, contact list, or similar information associated with the Subject Account.

f. Subscriber and payment information. All subscriber and payment information regarding the Subject Account, including but not limited to name, username, address, telephone number, alternate email addresses, registration IP address, account creation date, account status, length of service, types of services utilized, means and source of payment, and payment history.

g. Transactional records. All transactional records associated with the Subject Account, including any IP logs or other records of session times and durations.

h. Customer correspondence. All correspondence with the subscriber or others associated with the Subject Account, including complaints, inquiries, or other contacts with support services and records of actions taken.

i. Preserved records. Any preserved copies of any of the foregoing categories of records created in response to any preservation request(s) issued pursuant to 18 U.S.C. § 2703(f).

III. Review of Information by the Government

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by GitHub, Inc. in order to locate any evidence, fruits,

and instrumentalities of violations (i) the unauthorized possession and, *inter alia*, the communication of national defense information to someone not entitled to receive it, in violation of Title 18, United States Code, Section 793(d); (ii) the unlawful retention of national defense information, in violation of Title 18, United States Code, Section 793(e); (iii) exceeding authorized access to a computer in order to obtain national defense information with reason to believe that information could be used to the injury of the United States and the advantage of a foreign nation and willfully transmitting that information to a person not entitled to receive it, in violation of Title 18, United States Code, Section 1030(a)(1); and (iv) intentionally exceeding authorized access to a computer and thereby obtaining information from a department or agency of the United States, in violation of Title 18, United States Code, Section 1030(a)(2)(B) (collectively the "Subject Offenses"), including the following:

- w. Evidence of the identity(s) of the user(s) of the Subject Account as well as other coconspirators in contact with the Subject Account;
- x. Evidence relating to the participation in the Subject Offenses by the users of the Subject Account and others;
- y. Evidence concerning financial institutions and transactions used by the users of the Subject Account in furtherance of the Subject Offenses;
- z. Communications evidencing crimes, including but not limited to correspondence with others relating to the unauthorized retention, gathering, and transmission of classified documents or materials, and the unauthorized removal and retention of classified documents or materials;

- aa. Evidence of and relating to computers or other online accounts and facilities (such as additional email addresses) controlled or maintained by the user of the Subject Account; and
- bb. Passwords or other information needed to access any such computers, accounts, or facilities.

EXHIBIT B

Monday 8/27

Rewriting my articles I guess. If you want something done right you gotta do it yourself.

1-9, 10: Rewrite Material of the first into 4-5 pgs. So I have the originals which only need slight edits; [1, 2, 3, 6, 7, 8] - half.

I want to start the philosophy (class) with a photo & end with a bible quote. For ex.

#4: Victor Frankenstein

#7: Kill all the Hungers, Shakespeare, Macbeth?

4: written, just needs to be retyped 15 pgs.
5: written, just needs to be retyped 20 pgs.
8: written, just needs to be retyped
9: written, just needs to be retyped
10: needs to be written

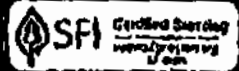
1 3 5 7 9 - Should all be my story.

2 4 6 8 10 - All philosophy.

- BUT - > Snapped. Snap back?

EXHIBIT C

NEAT SHEET



Mead.
Learn. Organize. Create.

**1 SUBJECT
WIDE RULED**

Assembled in U.S.A.



wireless
NEATBOOK® NOTEBOOK

10 7/8 IN x 8 IN / 26.6 cm x 20.3 cm

**80
SHEETS**

GOVERNMENT
EXHIBIT
809
5247 CH 648 (PAC)

If you don't pay me \$50 billion in restitution to prosecute the criminals who lied to the judge and presented this as a case for I will visit every country on the world and hear witness to the treacher that is the USG. I will look to breakup diplomatic relationships, close embassies, and

Wednesday 8/8 2016

They called me down at 6AM for my 2PM conf. US. occupation across the world. From 6-10AM I did nothing down there. Finally brought me back. I took my last piece of I'm feeling great. I envisioned my appointment as a Cardinal and becoming the Pope as I finally unified Christianity around the Church. reverse US. English. Don't if this is the way the US. got that one of the duty here so you think they treat others?

Took too much to feel sick. 11

Presumption of Innocence
A Redress of Grievances

Joshua Schulte
Indefinitely Incarcerated
Inmate Estate

1 charge per day
1x from 3-death

Tuesday 8/14

Inmate indefinitely increases through

Give me a
phone & a
blog & I
will
charge for
work

Got to use last night. The way is clear. I will
Setup a Wordpress of joshschulte.wordpress.com and
presumptionofinnocence.wordpress.com. From here, I
will stage my information war:

Facebook I will rename, simply, "Who is John Galt?"
"Who is Josh Schulte?"

From FB, I will post links to the articles and blogs as I
write them.

The presumption of innocence blog will only contain my
10 articles 1-10, ending on the presumption of innocence.
I will post each of them on the FB & delete the previous
articles

Although I was
only with the
company for a
short time,
it did feel like
a family to
me and I
am grateful to
those who
know me

From my blog, I will write about my times etc.

I am grateful to my Bloomberg Friend for facilitating my voice.
Perhaps one of the ~~most~~^{most} aspects of federal prison is the
inability to defend yourself as the Federal Government unleashes its
disinformation blitzkrieg. That ends today. I want the world
to learn what has happened over the past year: The United States
Federal Government is the most corrupt, tyrannical government on
the planet. No person, or entity, or other govt
were bodies & heads themselves to my assistance can escape its bullying grasp.

I text my Dad from whatsapp & Signal messently & finally got a response @ 1% battery. I said please put articles on drafts in gmail. Response: My lawyer advised me not to. Fucking terrible. Fucking. Incredible. My own father, who forced me into \$150,000 of credit card debt wont help me. Why the fuck is everyone such a god damn pussy. **EVERYONE IS SO FUCKING PUSY!** Grow a pair and stand up to these assholes.

Was finally able to call & talk to him and it felt so fucking bad. The man sounded terrified at the govt & said they're watching my email, they're listening & watching everything. But, he also said Josh Drake was coming to see me today or fri. I thought I convinced him to setup a protonmail email acct for me to upload the articles

Tuesday 21st

They got smt
of my phone
via subpoena
at phone #

- ✓ 1.) Delete all Google Docs from johnsmith
- 2.) Delete all emails from johnsmith
- 3.) Delete suspicious emails from my gmail
 - a.) New logins from phone
 - b.) Paypal
 - c.) Wordpress
 - d.) PW changes
- ✓ 4.) Create new protonmail: protonedguilty@protonmail.com
- 5.) Migrate Wordpress to protonmail

Research

- 1.) Gmail keep deleted emails?
- 2.) Charging Sensors IMEI
 - a.) without rooting
 - b.) Generate new IMEI

Subpoena for IMEI?
Worst cases all 3
have compromised
IMEIs

- 6.) Clean off apps
- Reset factory phone

— New phone uses old
phone's whatsapp?

— Need to setup
Whatsapp with non-
Call number.

Setup whatsapp signal
telegram all with different
numbers!

capital &

786456

SR@S@Z/Jg7E59X^ <presumed guilty@
protonmail

Whats app FB Dads orbit
Signal WP Proton turbo VPN
Urm Oltex Apps

Subj 7366

[annon1204 g86ky24] made 56-12
jcha12gall21
@gmail.com

Subj 7366

\$ free-jason-bonne 1.138EF\$X

Jason Bonne gmail: V864LE50

Jiliasp@747965@outlook
Passwprid 69

sn 73 pr V69

The Lean Startup

Thursday August 23rd

Vestuday
Well a lot has happened lately. ~~Tuesday~~ I started
closing the phone in the process setup a new
gmail which I transferred the Wordpress too. I
also noticed that no mgs were responded on whatsapp
so I asked my bro. he went back and forth but they
decided for me not to publish the articles - hell, rather
not to give me my own fucking articles. Isn't that
mendable? They started up to begin with & published
the wrong (old) versions. Then they didn't publish
the two most important parts (B & C) and now they
are withholding ALL of them.

Heard tonight from my parents that Josh Patel
is coming tomorrow, mid-morning... 9, 10 AM

Yesterday I started emailing Steve from the
Washington Post

940-264-0825

Shane Harris 202-464-4827

just plan
call

send email: shane.harris@graher.com

I'm hoping to write/edit my portfolio. I don't know
how I can get this -- oh I may text Shane Harris
from Shane Harris's number. Don't think that you would
expect to do this -- I'm not sure.

Although I feel this may
not work either. IDK. Basically on hold for my
publication.

Secondly, I want to rewrite article #10: Volume of the
Mind!

... find Casini's book intro (edit).

I want to finish reading BOTH "The New Jim Crow" & "Victor
Francis"

Schultz was
the higher
representative

Amir - Azerbaijan
Alina, Turkey -- [USG acknowledges coup attempt]
(classified information)

half of
USG

Reality Winner

log from vendor report

Don't know for

vendor

Mark Sander
Thomas guy

China & Russia openly attacking us
looking to undermine world reserve currency

CVSB

Tried to outbid the first.

Map with to look

The CIA was in charge of [redacted]
[redacted] the CIA [redacted] placed
under operation [redacted] [redacted]
[redacted] [redacted] [redacted] [redacted]

of [redacted] [redacted] [redacted]
[redacted] [redacted] [redacted] [redacted]
[redacted] [redacted] [redacted] [redacted]

new [redacted] [redacted]
[redacted] [redacted] [redacted] [redacted]
[redacted] [redacted] [redacted] [redacted]

File 7

Don't get me wrong, [redacted] [redacted] [redacted]
[redacted] [redacted] [redacted] [redacted] [redacted]
[redacted] [redacted] [redacted] [redacted] [redacted]
[redacted] [redacted] [redacted] [redacted] [redacted]

He can control [redacted] [redacted] [redacted]
[redacted] [redacted] [redacted] [redacted] [redacted]

Spe. [redacted]

the Red Donald Trump [redacted] [redacted] [redacted]
[redacted] [redacted] [redacted] [redacted] [redacted]
[redacted] [redacted] [redacted] [redacted] [redacted]
[redacted] [redacted] [redacted] [redacted] [redacted]

The [redacted]
[redacted] [redacted] [redacted]

[redacted] [redacted] [redacted] [redacted] [redacted]
[redacted] [redacted] [redacted] [redacted] [redacted]

I don't know about the [redacted] [redacted] [redacted]
[redacted] [redacted] [redacted] [redacted] [redacted]
[redacted] [redacted] [redacted] [redacted] [redacted]
[redacted] [redacted] [redacted] [redacted] [redacted]
[redacted] [redacted] [redacted] [redacted] [redacted]

1

He dated [redacted] [redacted] [redacted]
[redacted] [redacted] [redacted] [redacted] [redacted]
[redacted] [redacted] [redacted] [redacted] [redacted]
[redacted] [redacted] [redacted] [redacted] [redacted]

Establish credibility

It's not #1. It's Top Secret.

attempted.

→ on the way to the server here!

Let me first ~~authenticate~~ myself. The user was
induced in the [REDACTED]

[REDACTED] Same code for the
released [REDACTED] cyber espionage component is in the Vault /
Release.

The CIA conducted various operations against [REDACTED] and

[REDACTED]

Same code is available in the Vault 7 release

@vendor discussed tool [REDACTED] is really what is really for

CIA's Executive team [REDACTED]

Barber was written [REDACTED]

[REDACTED] to deploy against various targets. This same
code is available in the Vault 7 release.

Lastly

Vault 7 contains numerous zero-days and malware that
could be deployed, repurposed and the released code the
involved in a devastating fashion that would make that getting
into the child's play. [REDACTED]

[REDACTED]

My notes

200
Rosa
Street
Nashville
10007

To the United States Intelligence Community - why build
this crap? ~~After 9/11, we spent a lot of money on this crap~~
~~for our country~~ ~~prevents your own?~~

Yolby Gilder
Harrisburg, PA

The Dept of Justice arrested the wrong man for 9/11.
I personally know exactly what happened as do many
others - why are they covering it up?

Jeremy Weber

Meet the CIA's own spy: ~~Mark~~
~~Karen~~ ~~Wright~~ (you can find his info in the Ashley Madison
dump) and Karen ~~Wright~~ setup Josh Schulte.

→ The Service, not intense security investigations, and passive. Criminal history
 can mean not your bail. As John Schiller has said, you are
 bound a presumption of innocence. If not, you do your country's
 dirty work. But when your country accuses you of a crime, you
 are arrested & presumed guilty. Until your country pardons you
 all your god's enemies here! Look! Look! But

→ This is a HELL: walk-up call to U.S. intelligence officers.
 The Constitution you fight to defend will be denied to you
 if, God forbid, you are ever accused of a crime. If your country
 has no allegiance, in that way to you have any allegiance
 than for you?

(our associates provided info to the USF)

Can you change a cell phone with pictures?

For King

September 2, 2018

Well it's September now. I've been in all day. Hopefully tonight I can setup Signal from my cell & msg. I'll be working my damn perimeter and get my fucking caries. I also need to combine my teeth.

Personnel - Hedge Fund. With a little Jack Capital

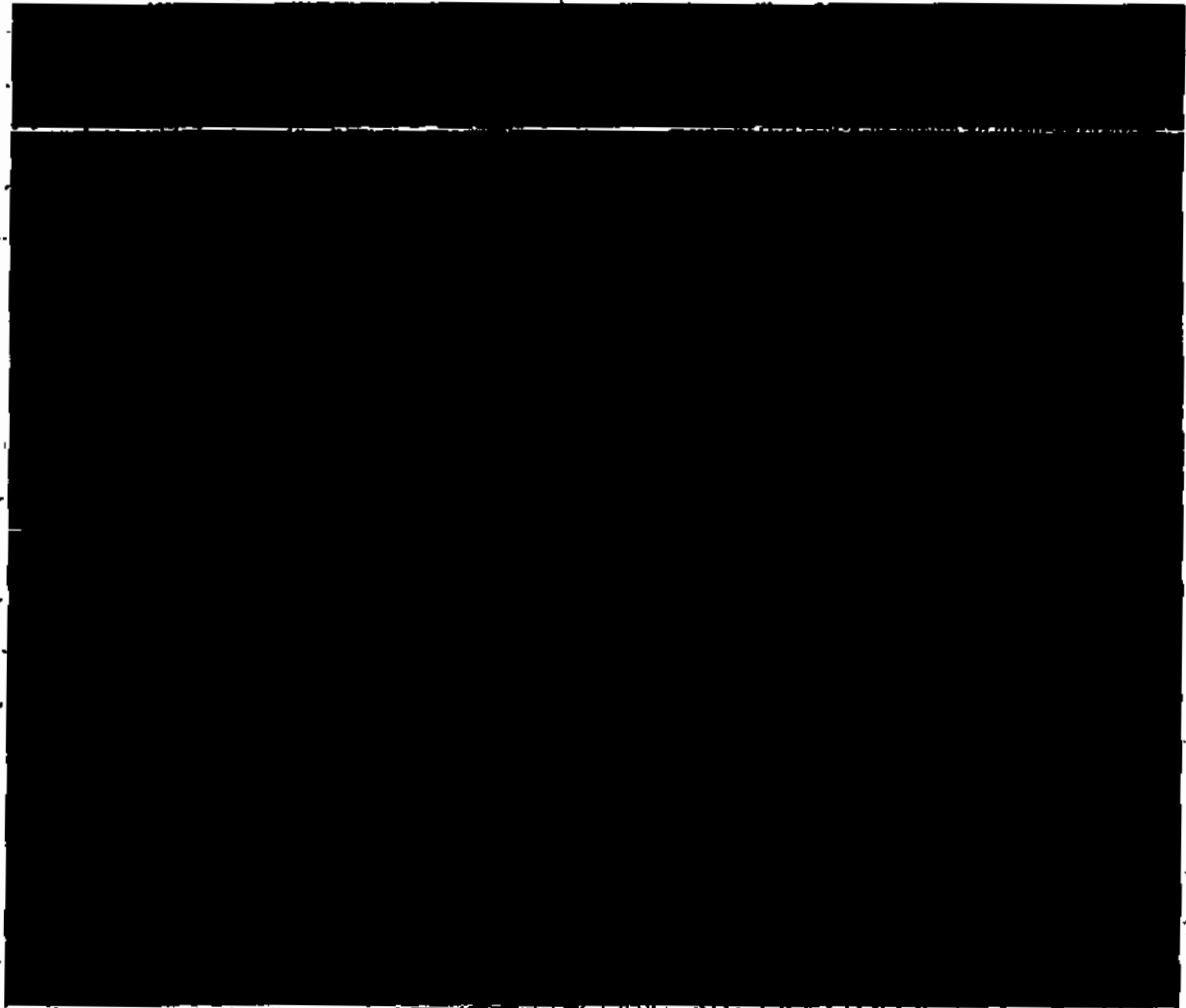
Thomas Mann, The Magic Mountain

| | |
|------|------|
| 4.1 | 2.85 |
| 4.2 | 2.85 |
| 4.3 | 2.85 |
| 4.4 | 2.85 |
| 4.5 | 2.85 |
| 4.6 | 2.85 |
| 4.7 | 2.85 |
| 4.8 | 2.85 |
| 4.9 | 2.85 |
| 5.0 | 2.85 |
| 5.1 | 2.85 |
| 5.2 | 2.85 |
| 5.3 | 2.85 |
| 5.4 | 2.85 |
| 5.5 | 2.85 |
| 5.6 | 2.85 |
| 5.7 | 2.85 |
| 5.8 | 2.85 |
| 5.9 | 2.85 |
| 6.0 | 2.85 |
| 6.1 | 2.85 |
| 6.2 | 2.85 |
| 6.3 | 2.85 |
| 6.4 | 2.85 |
| 6.5 | 2.85 |
| 6.6 | 2.85 |
| 6.7 | 2.85 |
| 6.8 | 2.85 |
| 6.9 | 2.85 |
| 7.0 | 2.85 |
| 7.1 | 2.85 |
| 7.2 | 2.85 |
| 7.3 | 2.85 |
| 7.4 | 2.85 |
| 7.5 | 2.85 |
| 7.6 | 2.85 |
| 7.7 | 2.85 |
| 7.8 | 2.85 |
| 7.9 | 2.85 |
| 8.0 | 2.85 |
| 8.1 | 2.85 |
| 8.2 | 2.85 |
| 8.3 | 2.85 |
| 8.4 | 2.85 |
| 8.5 | 2.85 |
| 8.6 | 2.85 |
| 8.7 | 2.85 |
| 8.8 | 2.85 |
| 8.9 | 2.85 |
| 9.0 | 2.85 |
| 9.1 | 2.85 |
| 9.2 | 2.85 |
| 9.3 | 2.85 |
| 9.4 | 2.85 |
| 9.5 | 2.85 |
| 9.6 | 2.85 |
| 9.7 | 2.85 |
| 9.8 | 2.85 |
| 9.9 | 2.85 |
| 10.0 | 2.85 |

"A long-filled & hopeless striving of life for
 comfort and ease, but when we are beginning to
 find that it does not - ultimately to be used,
 some other must be substituted to compensate,
 because it is unable to live for itself."

disguise as a tech guy
in Florida

Wed 9/12



Finalize copy by Friday
Edit during weekends Sat, Sun; Finalize
Monday 17th - Tues 18th; DL Disc, VL WL
19, 20, 21; Schedule tweets 27th; Send tech report MCL letter,
Russia press)
Rest 22-25

Monday 4/17

* Still got to turn in
6:45 off 109.125
* (109) 600
*

Don't have been sleeping the last few nights so I've
gotten great sleep. This morning I slept until
like 9:30 AM straight. No chance to be anything
in the morning.

Talked with Belum today from 6 to 7ish or
so. He's an interesting, old man. Loved his music.
I'll be happy once he jumps on board — him & Mark.
Seiden will make a great team.

I posted the FB thing — on the John. Don't
page & changed the pic. We'll see what happens.
Probably a little interest. In a week I'm going to
dump all my stuff.

Tech report still missing. Or editing, game
stuff, etc. Should be able to finalize by ~~the~~ tomorrow.
Then Wednesday the mail & off to W. Po.

My printer is having trouble with the
photo. 100% 102; Apparently I can get it done
today for release on the 25th but maybe not?

EXHIBIT D

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

-v-

JOSHUA ADAM SCHULTE,

Defendant.

S3 17 Cr. 548 (PAC)

**DECLARATION OF JOSHUA ADAM SCHULTE IN SUPPORT OF
DEFENDANT'S MOTION TO SUPPRESS MALWARE OF THE MIND**

Joshua Adam Schulte declares under penalty of perjury:

1. I wrote Malware of the Mind in March of 2018 exclusively for my NEW attorneys from the Federal Defenders. The title of the document derived from a paragraph first written in my technical report for Omar Amanat; this paragraph was subsequently included in the opening paragraph for Malware of the Mind. As is the case with all attorney-client work product and privileged information, I wrote Malware of the Mind in a narrative format—the government previously seized several attorney-client privileged documents dating back to March of 2017 in which I wrote information for my attorneys in a narrative format, but which was never published or ever intended to be published, thereby confirming my testimony.
2. After finishing with the document, I mailed/transferred it to Hannah Sotnick, a paralegal with the Federal Defenders of New York, asking her to give it to my counsel and to give me any advice about the document. She made copies and distributed it to my attorneys. She then mailed me back both the original

and a copy that contained hand-written commentary from either her or another representative from the Federal Defenders (this commentary can be found on the government's seized photocopy). The copy was incomplete, and I asked her if she could make another copy. She then made a complete copy and mailed me the missing pages while maintaining the original.

3. That photocopy of *Malware of the Mind* remained inside the Federal Defenders envelope it was mailed in from the time it was received in March 2018 until FBI Agent Donaldson executed his unconstitutional general warrant of the MCC, seized the envelope marked as attorney-client privileged, opened it, and then read the entire document although the warrant did not identify *Malware of the Mind* to seize.
4. After the government falsely claimed *Malware of the Mind* was "classified," my attorneys brought the original to the SCIF in an abundance of caution, where it remains to this day. The government's seized photocopy would perfectly match the original document that remained in my attorney's possession as it was written exclusively for them. *Malware of the Mind* was sent to no one else.
5. Half a year after *Malware of the Mind* was written, I contemplated a tenth and final article in my *unclassified* redress of grievances criticizing the federal government and its corrupt criminal justice system. As I always liked the title "*Malware of the Mind*" and the associated paragraph first written in the Omar Amanat technical report, I considered reusing this as the opening paragraph for the final article. However, as my articles are about the corrupt, diabolical American criminal "just us" system, the content would obviously differ completely. This is why page 125 of "*Red Notebook - Gen 7.25-9 - UNCLASSIFIED*" (2019.05.29 production) AND Ex. J (Trial Exhibit 809 p. 8; Tr. 2525) states "rewrite *Malware of the Mind*." Ultimately, I scrapped

the idea for a tenth article entirely as I felt the nine were sufficient for my purposes.

6. Accordingly, the "Malware of the Mind" illegally seized and searched by Agent Donaldson was drafted for, and only ever transmitted to, my attorneys, for the express and sole purpose of aiding my criminal defense.
7. Finally, I testify that page 84 of 145 of Malware of the Mind is not National Defense Information nor is it even classified. With six years of experience with classified information, the key is specificity; keeping something generic keeps the information unclassified. When I wrote page 84 of 145 not only did I *not* intend any harm to the United States, but I specifically rewrote the section multiple times in an attempt to ensure it was generic and therefore completely unclassified. These extra efforts to ensure no classified information was compromised definitively prove that there was never any attempt to harm the United States.
8. This information relating to [REDACTED] is very generic, and based upon public knowledge dating back millennia. I intended the information to be generic, and did not reveal specific information about specific CIA products [REDACTED]. The information as written could not be used to identify any CIA malware that I wrote, worked on, or knew about in my time at the CIA.

I declare under penalty of perjury that the foregoing is true and correct.

Dated: New York, New York

January 24, 2022

Joshua Adam Schulte, *pro se*

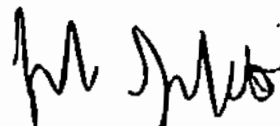


EXHIBIT E-1

MALWARE of the MIND

| | |
|---|-----|
| Introduction..... | 1 |
| Transcripts..... | 5 |
| The Search Warrant..... | 43 |
| The Complaint..... | 59 |
| Ethics and a LOGICAL look at the charges..... | 87 |
| Tyranny..... | 109 |
| Conspiracy..... | 121 |
| Conclusion..... | 133 |

1

Introduction.

Today, we are facing a stealth Constitutional crisis. A malware of the mind has entered and corrupted the justice system. Technology has advanced so rapidly that the law and law enforcement are decades behind and are unable to catch-up. Into this chasm, defendant, defense lawyers, judges, and juries are increasingly blind-sided by the evolution of innovative prosecutorial techniques based on faux forensics, manipulation, and intentional misrepresentation which are in turn nothing more than longshot theories and in some cases blatant fabrication: analogous to accusations of witchcraft and witchdry.

To my fellow engineers and the tech industry: The United States of America has corrupted and perverted our creations to serve their own manipulative purposes. We must intervene and prevent the malicious FBI and federal authorities from deceiving judges and juries regarding technology that was never intended for use in the court of law or to definitively ascertain culpability. Your very users are at serious threat of prosecution for simply using your services — services like Google Searches are declared to be definitively the account user's searches and subsequently used against them in the court of law as they are incredibly held criminally liable; Entire digital footprints are collected and data cherry-picked to depict

2

an ~~infinite~~ individual as a monster — This "FBI Challenge", as I dub it enables the FBI free reign over technology and our data to manipulate and persecute anyone they desire. For example, I have always allowed massive collection and storage of my electronic information. I created my gmail account back in high school around 2006, and since then I have retained all my information. I enabled all google... geotagging, location scanning, google search history, google voice, and the backup of all texts via email, and I literally opted in to almost every service to collect my data. I've used all of Google's products from their desktop Google Maps, Google Reader, to Google domains, Google email and site management, Google's Nexus One, etc. I've also used several other platforms outside Google as well. This sounds contrary to the advice of most security experts (I never recommended anyone to do as I did), but I found the technology involved fascinating and was interested from an offensive, malware developer's perspective. It was also interesting to possess the ability to review where I was, what I was searching, and my interests from an instantaneous viewpoint in the past. Once I was an old Grandpa, I could look back and reminisce over 30 yrs of data that was essentially the very digital representation of my important self. Anyway, I already worked for Big Brother and felt little real concern regarding the solicitation of my personal data. HOWEVER, I left the CIA — And I never anticipated the possibility that my own government

3

Would manipulate and dishonestly cherry pick and mislead this massive data to paint me as a monster. Of the hundreds of millions, or even billions of digital data points such as searches, emails, texts, pictures, location data, chats, posts, blogs, etc over the span of 12+ years, the FBI cherry pick 3 data points here or 2 there and ignore all the innocuous data to fit their own narrative; Data taken out-of-context or even falsely attributed to me. They say there are lies, damned lies, and statistics — but then there is the FBI; they manipulate statistics and corrupt technology for their own malevolent end.

And so this final article is the coup de grace. I have mostly discussed the problems with the justice system in general, but here I will target one of the growing threats to justice: Technology. Judges are almost entirely old and thus have no concept or understanding of technology at all. Our legal system is the upside-down; here, there are no adults in the room. No tech experts sitting beside the old, senile judges to untangle the lies and deception woven by the FBI and prosecutors. No intelligent, unbiased individuals to inform and instruct judges what to do.

And so we will embark on my journey through the upside-down where there is no logic or intelligence; left is right, up is down, war is peace, and idocracy and malfeasance

4

run rampant.

5

Transcripts

To begin, we'll start with the incredible prejudice against technology and technical people. The United States of America hawks people with engineering degrees and technical expertise to be a danger to society; if you possess technical knowledge that be wary — America will come for you. The prosecutor will inform the judge of your knowledge and it will be used against you in the court of law.

Here is the incredible incompetence, prejudice, and incorrigible behavior of the United States prosecutor & judge in REAL LIFE official court transcripts:

6 Bail Hearing #1

ROACH: And even more critical evidence, the defendant has already admitted that this computer was his. He admitted that no one else used it. He admitted that he was the one who transported it. And he has admitted that he is the one in the IRC chat. So there's really no dispute --

Magistrate: He is the one in the chat?

ROACH: I'm saying, your honor, the IRC chats that are cited in the Complaint.

Magistrate: What does IRC stand for?

ROACH: You know, I'm not sure offhand, your Honor, but my understanding is it's a program that you can download onto your computer, which is basically like a chat that you can chat back and forth with.

ROACH: With respect to the history and characteristics of the defendant, I want to focus on two things that he thinks particularly support detention here. First, the defendant is highly sophisticated when it comes to computers. That's shown not just with how he stored this information but also his background. Up until today he was employed as a senior software engineer for Bloomberg. Before that,

7

he worked for several years for various government agencies where he had similar roles. He has expertise and experience in encryption. He has expertise and experience in using tools such as wiping tools, which essentially deletes any evidence that someone went to certain websites, accessed certain things, may have looked at certain images or videos. So he absolutely knows how to hide his tracks, and I think it shows by the level of the carefulness he took.

PDAH:

Sure, you know. Well, he's already secured another computer. So as of today when they went into his apartment, he has another computer that he's already gotten and has already had - we assume have various programs on.

The problem here is that his expertise makes it very difficult to be able to detect any additional conduct by him in terms of downloading these images or continuing in the same type of conduct that he has done for years.

And just one thing to note, in March, when the officers went to his apartment, it wasn't as though he had one computer. This defendant, we believe, his identity is really tied to computers and electronic devices. He had numerous computers, servers, other storage equipment.

Magistrate: How many computers?

LOPEZ: So he had one desktop computer, your Honor, but he had a number of servers and other storage devices that could store over 10 terabytes of data. It's an enormous amount of data that the government is still continuing to work through. So we don't even know yet if we've gotten the full cache of images that could be on this defendant's computer.

And part of the difficulty with this is that the defendant is sophisticated enough to be able to create data files that virtually are undetectable. And it's been very difficult to get through that entire cache of data. So he has some sophistication to be able to do this, whether it's his computer or if he gets another computer after, if he was to be released. We just do not think there's any set of conditions that would prevent that risk.

ROACH: Beyond simply being a danger, your Honor, we believe that he is a flight risk. The defendant, as of today, is unemployed. He has very few contacts to New York City otherwise. He's also facing charges which carry a mandatory minimum term of five years. By the way we calculate his Guidelines, we think he'd probably be close to the statutory max here. So he has a strong incentive, based on the weight of the evidence and the length of sentence he's facing, to flee.

So in sum we just don't think that there are a set of conditions here that can ensure that he is going to appear in court or not be a danger to the community and need ask.